SANbox 6142
Intelligent Storage Router

User's Guide

FI0054601-00 C

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

This SANbox switch is covered by one or more of the following patents – 6697359; other patents pending.

QLogic and SANbox are trademarks or registered trademarks of QLogic Corporation.
AMCC is a registered trademark of Applied Micro Circuits Corporation
Brocade is a registered trademark of Brocade Communications Systems, Inc.
Cisco is a registered trademark of Cisco Technology, Inc.
Gnome is a trademark of the GNOME Foundation Corporation.
Java and Solaris are registered trademarks of Sun Microsystems, Inc.
Pentium is a registered trademark of Intel Corporation.
IBM and PowerPC are registered trademarks of the International Business Machines Corporation.
Linux is a registered trademark of Linus Torvalds.
MacOS X and Safari are registered trademarks of Apple Computer, Inc.
McDATA is a registered trademark of McDATA Corporation.
Microsoft, Windows XP, Windows 2003, and Internet Explorer are registered trademarks of Microsoft Corporation.
Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.
Red Hat is a registered trademark of Red Hat Software Inc.
SANmark is a trademark of the Fibre Channel Industry Association.
SUSE is a trademark of Novell, Inc.
All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Revision B

Changes	Sections Affected
Edited and updated format to new QLogic style 03/08	Entire Book
Updated illustrations of SANbox 6142 router box	Sections 2 and 5
Corrected information about Heartbeat vs System Fault LEDs	Section 2
Clarified instructions for pressing the maintenance button	Section 2

© 2008 QLogic Corporation. All Rights Reserved Worldwide.
Published: Month Year

QLogic Corporation, 26650 Aliso Viejo Parkway, Aliso Viejo, CA 92656, (800) 662-4471 or (949) 389-6000

Removed reference to SANsurfer application installation from a CD; replaced CD installation procedures with steps for downloading software from the QLogic website	Section 4
Corrected information about when the Configuration Wizard launches automatically	Section 4
Corrected information on LED diagnostics to identify the blink patterns that display on the System Fault LED, not the Heartbeat LED	Section 5
Updated screens and descriptions regarding IP addresses to include IPv6 options in SANsurfer iSCSI/FC Router Manager	Section 7
Added `traceroutes` command and replaced screen samples to show IPv6 support	Appendix A

Notes

Table of Contents

1 Introduction

Intended Audience 1-1
Related Materials 1-1
Safety 1-2
Communications Statements 1-2
Federal Communications Commission (FCC) Class A Statement . . . 1-3
Canadian Department of Communications Class A Compliance Statement 1-3
Avis de conformité aux normes du ministère des Communications du Canada 1-3
CE Statement 1-4
VCCI Class A Statement 1-5
Laser Safety Information 1-5
Electrostatic Discharge Sensitivity (ESDS) Precautions 1-5
Accessible Parts 1-6
License Agreements 1-6
General Public License 1-6
Preamble 1-6
Terms And Conditions For Copying, Distribution and Modification . . . 1-7
How to Apply These Terms to Your New Programs 1-13
Technical Support 1-14
Availability 1-14
Training 1-14
Contact Information 1-14

2 General Description

Router Capabilities 2-2
Licensed Features 2-2
SmartWrite 2-2
Additional Server/Ports 2-3
Remote SAN Island Connectivity 2-4
Local SAN Island Connectivity 2-6
FCIP - Fibre Channel over IP 2-6
Chassis LEDs 2-7

Heartbeat LED (Green) . . . 2-7
Input Power LED (Green) . . . 2-7
System Fault LED (Amber) . . . 2-7
Chassis Controls . . . 2-8
Maintenance Button . . . 2-8
Reset a Router . . . 2-8
Reset and Select Boot Image . . . 2-9
Reset IP Address . . . 2-9
Enable DHCP . . . 2-9
Restore Factory Defaults . . . 2-9
Fibre Channel Ports . . . 2-10
Fibre Channel Port LEDs . . . 2-10
Fibre Channel SFP Transceivers . . . 2-11
iSCSI/Gigabit Ethernet Port LEDs . . . 2-12
Ethernet Port – Management . . . 2-12
Serial Port . . . 2-13

3 Planning

Devices . . . 3-1
Device Access . . . 3-2
Fibre Channel . . . 3-2
iSCSI . . . 3-2
FC Performance . . . 3-2
Distance . . . 3-2
Bandwidth . . . 3-3
Latency . . . 3-3
iSCSI/Gigabit Ethernet Performance . . . 3-3
Distance . . . 3-3
Performance Tuning . . . 3-3
Topology . . . 3-7
Fibre Channel Switch Ports and Zoning Requirements . . . 3-8
Multiple Routers . . . 3-8
Management . . . 3-8
Recovery . . . 3-8
Services . . . 3-9
Security . . . 3-9

4 Installation

Site Requirements 4-1
Management Workstation 4-1
Power Requirements 4-2
Environmental Conditions 4-2
SANbox 6142 Router Installation 4-2
Pre-installation Check List 4-4
Mount the Router 4-4
Install the Transceivers 4-5
Connect the Management Workstation to the Router 4-5
Configure the Management Workstation 4-5
Setting the Workstation IP Address 4-6
Configuring the Workstation Serial Port 4-6
Install SANsurfer iSCSI/FC Router Manager 4-7
Windows Installation 4-7
Linux Installation 4-8
Start SANsurfer iSCSI/FC Router Manager 4-8
Connect the Router to AC Power 4-9
Configure the Router 4-10
Cable Devices to the Router 4-11
Firmware Installation 4-11
Using SANsurfer iSCSI/FC Router Manager to Install Firmware 4-11
Using the CLI to Install Firmware 4-12

5 Diagnostics and Troubleshooting

Chassis Diagnostics 5-1
Input Power LED is Off 5-2
System Fault LED is On 5-2
Power-On Self-Test Diagnostics 5-2
LED Blink Patterns 5-3
Heartbeat Blink Pattern 5-3
System Error Blink Pattern 5-3
Management Port IP Address Conflict Blink Pattern 5-4
Over-Temperature Blink Pattern 5-4
Recovering a Router 5-5

6 Removal/Replacement

SFP Transceiver Removal and Replacement 6-1
Router Removal and Replacement 6-2
Removal 6-2
Replacement 6-2

7 SANsurfer iSCSI/FC Router Manager

Introduction. 7-1
Menu Bar 7-3
File Menu. 7-4
View Menu. 7-4
Settings Menu 7-4
Wizards Menu 7-5
Help Menu 7-7
Tool Bar 7-7
Action Menu. 7-8
System Tree Window 7-10
SANbox 6142 Router. 7-12
Information Tab. 7-12
SNMP Management Tab 7-17
Features Tab. 7-19
Assigned Remote Router Tab. 7-19
Topology Tab 7-20
FC Ports 7-20
FC Port Information Tab 7-21
FC Port Advanced Configuration Tab 7-21
FC Port Performance Tab. 7-22
iSCSI Ports 7-23
Information Tab. 7-24
Advanced Configuration Tab 7-27
Statistics Tab. 7-30
Discovered iSCSI Initiators 7-31
Information Tab. 7-31
Local Presented Target Tab 7-32
Remote Presented Target Tab 7-33
FC Discovered Targets 7-34
Information Tab. 7-35
Remote Presented Devices Tab. 7-35
iSCSI Presented Target List Tabbed Page 7-36

iSCSI Discovered Targets 7-38
Information Tabbed Page 7-38
FCIP Routes 7-39
FCIP Route Information Tabbed Page 7-40
FCIP Route Statistics Tabbed Page 7-42
Wizards 7-43
Configuration Wizard 7-44
Add Initiator Wizard 7-49
FW Update Wizard 7-51
Map Local Initiator/Target Wizard 7-55
Unmap Local Initiator/Target Wizard 7-63
Add Remote Router Wizard 7-68
Remove Remote Router Wizard 7-72
Map Remote Initiator/Target Wizard 7-75
Unmap Remote Initiator/Target Wizard 7-81
Discover iSCSI Target Wizard 7-84
FCIP Route Add Wizard 7-86
FCIP Route Remove Wizard 7-92

A Command Reference

Logging On to a SAN Router A-1
Guest Account A-2
Working with SAN Router Configurations A-2
Modifying a Configuration A-2
Saving and Restoring Router Configurations A-2
Save Router Configuration and Persistence A-3
Restore Router Configuration and Persistence A-4
Commands A-5
Admin Command A-6
Beacon Command A-7
Clear Command A-8
Date Command A-9
FcipRoute Command A-10
FRU Command A-13
Help Command A-14
History A-16
Image Command A-17
Initiator Command A-18
Localmap Command A-20
Logout Command A-23

Password Command A-24
Ping Command A-25
Quit Command A-26
Reboot Command A-27
Remote Map Command A-28
Remote Peer Command A-32
Reset Factory Command. A-34
Save Command. A-35
Set Command A-37
Set CHAP Command. A-39
Set FC Command A-40
Set Features Command A-41
Set iSCSI Command A-42
Set iSNS Command A-44
Set Mgmt Command A-45
Set NTP Command A-46
Set Properties Command A-47
Set SNMP Command A-48
Set System Command. A-50
Show Command A-51
Show CHAP Command. A-54
Show FC Command A-55
Show FcipRoutes Command. A-56
Show Features Command. A-57
Show Initiators Command A-58
Show iSCSI Command A-59
Show iSNS Command. A-61
Show Localmaps Command A-62
Show Logs Command A-63
Show Memory Command A-64
Show Mgmt Command A-65
Show NTP Command A-66
Show Performance Command A-67
Show Presented Initiators Command A-69
Show Presented Targets Command A-70
Show Properties Command. A-72
Show Remotemaps Command A-73
Show Remotepeers Command A-74
Show SNMP Command. A-75

Show Stats Command A-76
Show System Command A-79
Show Targets Command A-80
Show VLAN Command A-81
Shutdown Command A-82
Target Command A-83
Traceroute Command A-84

B Log Messages

Log Data B-1
Informational Log Messages B-1
Application Modules B-1
iSCSI Driver B-4
Fibre Channel Driver B-5
User Modules B-6
FCIP B-8
TOE Driver B-9
System B-9
Error Log Messages B-10
Application Modules B-10
iSCSI Driver B-18
Fibre Channel Driver B-20
User Modules B-22
System B-25
Fatal Log Messages B-25
iSCSI Driver B-25
FC Driver B-28
TOE Driver B-30
System B-31

C Configuring CHAP

CHAP Definition C-1
Configuring CHAP Using CLI C-1
CLI—Discovery Session—Bi-directional CHAP C-1
CLI—Discovery Session—Uni-directional CHAP C-2
CLI—Normal Session—Bi-directional CHAP C-3
CLI—Normal Session—Uni-directional CHAP C-4
Configuring CHAP Using the GUI C-4
GUI—Discovery Session—Bi-directional CHAP C-4
GUI—Discovery Session—Uni-directional CHAP C-5
GUI—Normal Session—Bi-directional CHAP C-6
GUI—Normal Session—Uni-directional CHAP C-7

D Simple Network Management Protocol (SNMP)

Introduction D-1
SNMP Properties D-1
SNMP Trap Configuration D-2
Management Information Base (MIB) D-3
System Information D-3
Network Port Table D-4
Fibre Channel Port Table D-6
Sensor Table D-8
Notifications D-11
Notification Objects D-11
Agent Start Up Notification D-11
Agent Shut Down Notification D-12
Network Port Down Notification D-12
Fibre Channel Port Down Notification D-12
Sensor Notification D-12
Generic Notification D-13

List of Figures

Figure		Page
2-1	SANbox 6142 Router	2-1
2-2	Remote SAN Island Connectivity	2-4
2-3	Local SAN Island Connectivity	2-5
2-4	Chassis LEDs	2-7
2-5	Chassis Controls	2-8
2-6	Fibre Channel LEDs	2-10
2-7	Gigabit Ethernet (iSCSI) Ports	2-12
2-8	Ethernet Management Port	2-12
2-9	Serial Port	2-13
3-1	LAN Topology - Local SAN Interconnect	3-7
3-2	WAN Topology - Remote SAN Interconnect	3-7
4-1	SANbox 6142 Router and Accessories	4-3
5-1	Chassis Diagnostic LEDs	5-1
7-1	SANsurfer Router Manager Main Window	7-2
7-2	Menu Bar	7-3
7-3	File Menu	7-4
7-4	View Menu	7-4
7-5	Settings Menu	7-4
7-6	Broadcast Settings Menu	7-5
7-7	Wizards Menu	7-5
7-8	Help Menu	7-7
7-9	Tool Bar	7-7
7-10	Action Menu	7-8
7-11	System Tree Window	7-10
7-12	Component Information	7-11
7-13	Basic Information Vertical Tab	7-12
7-14	Management Information Vertical Tab	7-13
7-15	NTP Server Information Vertical Tab	7-15
7-16	Security Vertical Tab	7-16
7-17	SNMP Management Tabbed Page	7-17
7-18	Features Tabbed Page	7-19
7-19	Topology Tabbed Page	7-20
7-20	FC Port Information Tab	7-20
7-21	FC Port Advanced Configuration Tab	7-21
7-22	FC Port Performance Tab	7-22
7-23	iSCSI Port Tabbed Pages	7-23
7-24	Advanced Configuration Tabbed Page	7-27
7-25	iSCSI Statistics Tabbed Page	7-30
7-26	Discovered iSCSI Initiator Tabbed Pages	7-31
7-27	Local Presented Target Tabbed Page	7-32
7-28	Remote Presented Target Tabbed Page	7-33
7-29	FC Discovered Targets Tabbed Pages	7-34
7-30	Remote Presented Devices Tab	7-35

7-31 iSCSI Presented Target List Tabbed Page . . . 7-37
7-32 iSCSI Discovered Targets Tabbed Pages . . . 7-38
7-33 FCIP Route Tabbed Pages . . . 7-39
7-34 FCIP Route Statistics Page . . . 7-42
7-35 iSCSI Port Selection Dialog Box . . . 7-44
7-36 iSCSI Port Connection Settings Panel Dialog Box . . . 7-45
7-37 iSCSI Port IPv6 Settings Panel . . . 7-46
7-38 Confirm Changes Dialog Box . . . 7-47
7-39 iSCSI Port Configuration Status . . . 7-48
7-40 Configuration Wizard Finish Dialog Box . . . 7-49
7-41 Create an Initiator Dialog Box . . . 7-50
7-42 Security Check Dialog Box . . . 7-50
7-43 System Tree with New iSCSI Initiator . . . 7-51
7-44 Router Selection Dialog Box . . . 7-51
7-45 Firmware File Selection Dialog Box . . . 7-52
7-46 Confirm Changes Dialog Box . . . 7-53
7-47 Security Check Dialog Box . . . 7-53
7-48 Firmware Update Status Dialog Box—Progress . . . 7-54
7-49 Finish Dialog Box (Successful Firmware Update) . . . 7-54
7-50 Initiator Selection Dialog Box . . . 7-55
7-51 Select a Target Dialog Box . . . 7-56
7-52 Select Initiator Port Dialog Box . . . 7-57
7-53 Select Target Presentation Port Dialog Box . . . 7-58
7-54 Confirm Changes Dialog Box . . . 7-59
7-55 Security Check Dialog Box . . . 7-60
7-56 Initiator/Target Mapping Configuration Status Dialog Box . . . 7-61
7-57 Discovered iSCSI Initiators - Local Presented Targets . . . 7-62
7-58 Initiator Selection Dialog Box . . . 7-63
7-59 Presented Target Selection Dialog Box . . . 7-64
7-60 Security Check Dialog Box . . . 7-65
7-61 Unpresent Initiator/Target Status Dialog Box . . . 7-66
7-62 Discovered iSCSI Initiators - Local Presented Targets . . . 7-67
7-63 Remote Router's IP Address Dialog Box . . . 7-68
7-64 Local Router Admin Password Dialog Box . . . 7-69
7-65 Add Remote Router Status Dialog Box . . . 7-69
7-66 Assigned Remote Router Display . . . 7-70
7-67 Topology Display . . . 7-71
7-68 Select Remote Router Dialog Box . . . 7-72
7-69 Local Router Admin Password Dialog Box . . . 7-73
7-70 Refresh Screen . . . 7-73
7-71 Remove Remote Router Completion Dialog Box . . . 7-74
7-72 Device Selection Dialog Box . . . 7-75
7-73 Device Selection Dialog Box . . . 7-76
7-74 Port Selection Dialog Box . . . 7-77
7-75 Device Mapping Option Dialog Box . . . 7-78

7-76 Confirm Mapping Dialog Box . . . 7-79
7-77 Local Password Dialog Box . . . 7-79
7-78 Local Router Admin Password Dialog Box . . . 7-80
7-79 Refresh Screen . . . 7-80
7-80 Remote Mapped Device . . . 7-81
7-81 Device Selection Dialog Box . . . 7-82
7-82 Local Router Admin Password Dialog Box . . . 7-83
7-83 Remote Unmap Initiator-Target Status Dialog Box . . . 7-83
7-84 Discover iSCSI Target Wizard—IP Address Dialog Box . . . 7-84
7-85 Discover iSCSI Target Wizard—Security Check Dialog Box . . . 7-84
7-86 Discover iSCSI Target Wizard—Refresh Dialog Box . . . 7-85
7-87 iSCSI Discovered Targets . . . 7-85
7-88 FCIP Route Add Wizard—Warning Dialog Box . . . 7-86
7-89 FCIP Route Add Wizard—Port Selection Dialog Box . . . 7-87
7-90 FCIP Route Add Wizard—Local and Remote IP Address Dialog Box . . . 7-88
7-91 FCIP Route Add Wizard—TCP/IP Options Dialog Box . . . 7-89
7-92 FCIP Route Add Wizard—FCIP Options Dialog Box . . . 7-90
7-93 FCIP Route Add Wizard—Security Check Dialog Box . . . 7-91
7-94 FCIP Route Add Wizard—Completed Dialog Box . . . 7-91
7-95 FCIP Route Remove Wizard—Warning Dialog Box . . . 7-92
7-96 FCIP Route Remove Wizard—Route Selection Dialog Box . . . 7-93
7-97 FCIP Route Remove Wizard—Security Check Dialog Box . . . 7-93
7-98 FCIP Route Remove Wizard—Completed Dialog Box . . . 7-94

List of Tables

Table **Page**

2-1 System Fault LED Blink Patterns . . . 2-7
2-2 Port LEDs . . . 2-10
2-3 Serial Port Pin Identification . . . 2-13
2-4 RJ-45 to DB-9 Adapter Pin Identification . . . 2-13
3-1 T1 / DS-1 – 1.554 Mbits/Sec . . . 3-3
3-2 T3 / DS-3 – 45 Mbits/Sec . . . 3-4
3-3 DS-5 – 400 Mbits/Sec . . . 3-4
3-4 OC-1 – 50 Mbits/Sec . . . 3-5
3-5 OC-3 – 150 Mbits/Sec . . . 3-6
3-6 OC-12 and Above – 621 Mbits/Sec . . . 3-6
4-1 Management Workstation Requirements . . . 4-1
4-2 Pre-installation Checklist . . . 4-4
5-1 System Fault LED Blink Patterns . . . 5-3
7-1 SANsurfer Router Manager Main Window Sections . . . 7-2
A-1 Command Line Completion . . . A-5
B-1 Application Modules—Informational Log Messages . . . B-1
B-2 iSCSI Driver—Informational Log Messages . . . B-4
B-3 Fibre Channel Driver—Informational Log Messages . . . B-5
B-4 User Modules—Informational Log Messages . . . B-6

B-5 FCIP—Informational Log Messages B-8
B-6 TOE—Informational Log Messages B-9
B-7 System—Informational Log Messages B-9
B-8 Application Module—Error Log Messages B-10
B-9 iSCSI Driver—Error Log Messages B-18
B-10 Fibre Channel Driver—Error Log Messages B-20
B-11 User Modules—Error Log Messages B-22
B-12 System—Error Log Messages B-25
B-13 iSCSI Driver—Fatal Log Messages B-25
B-14 Fibre Channel Driver—Fatal Log Messages B-28
B-15 TOE—Fatal Log Messages B-30
B-16 System—Fatal Log Messages B-31
D-1 SNMP Properties D-1
D-2 SNMP Trap Configuration Parameters D-2

1 Introduction

This manual describes the features and installation of the QLogic SANbox 6142 Intelligent Storage Router (iSR-6142), also referred to as the *SANbox 6142 router* or simply *router*.

Intended Audience

This guide is for users who are responsible for installing, managing, and servicing the SANbox 6142 router and the storage area network (SAN) equipment to which it is attached.

Related Materials

- *Internet Protocol, Version 6 (IPv6) Specification*., RFC2460.
- *Neighbor Discovery for IP Version 6 (IPv6),* RFC2461.
- *IPv6 Stateless Address Autoconfiguration*, RFC2462.
- *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*, RFC2463.
- *Transmission of IPv6 Packets over Ethernet Networks*, RFC2464.
- iSCSI draft standard draft-ietf-ips-iSCSI-20
- *Internet engineering task force (IETF) – iSCSI Requirements and Design Considerations, iSCSI Naming and Discovery, Internet Protocol Specification (IPv4)*, RFC793
- *Transmission Control Protocol (TCP) Specification, RFC1122, Requirements for Internet Hosts-Communication Layers*
- *TCP Extensions for High Performance*, RFC1323
- *TCP Congestion Control*, RFC2581
- *NewReno Modification to TCP's Fast Recovery Algorithm*, RFC2582
- ANSI SCSI – SCSI-3 Architecture Model (SAM), X3T10/994D/Rev 18, SCSI-3 Controller Command Set, X3T10/Project 1047D/Rev 6c. IEEE – 802.1Q Virtual LAN (VLAN), 802.1p Priority of Service, 802.3x Flow Control, 802.3ad Link Aggregation

- SCSI-3 Fibre Channel Protocol (SCSI-FCP), X3.269:1996
- Fibre Channel Physical and Signaling Interface (FC-PH), X3.230:199
- Fibre Channel 2nd Generation (FC-PH-2), X3.297:1997
- Third Generation Fibre Channel Physical and Signaling Interface (FC-PH-3), X3.303:1998, Fibre Channel-Arbitrated Loop (FC-AL-2), working draft, revision 6.4, August 28, 1998
- Fibre Channel Fabric Loop Attachment Technical Report (FC-FLA) NCITS/TR-20:1998, Fibre Channel-Private Loop Direct Attach Technical Report (FC-PLDA)
- SCSI Fibre Channel Protocol-2 (FCP-2) working draft, revision 3, October1, 1999
- Fibre Channel over TCP/IP (FCIP), RFC3821
- ANSI Information Technology-SCSI 3 Architecture Model, revision 18, November 27, 1995

Safety

WARNING!!

A **Warning** notice indicates a hazard that has the potential of causing minor personal injury.

CAUTION!

A **Caution** notice indicates the presence of a hazard that has the potential of causing damage to the equipment.

Communications Statements

The following statements apply to this product. The statements for other products intended for use with this product appear in their accompanying manuals.

Federal Communications Commission (FCC) Class A Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Neither the provider nor the manufacturer is responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Class A Compliance Statement

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

Avis de conformité aux normes du ministère des Communications du Canada

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

CE Statement

The CE symbol on the equipment indicates that this system complies with the EMC (Electromagnetic Compatibility) directive of the European Community (89/336/EEC) and to the Low Voltage (Safety) Directive (73/23/EEC). Such marking indicates that this system meets or exceeds the following technical standards:

- EN60950-1, A11:2004 – “Safety of Information Technology Equipment, Including Electrical Business Equipment”.
- EN 55022:1998, A1:2000, A2:2003 – “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment”.
- EN 55024:1998, A1:2001, A2:2003 – “Electromagnetic compatibility - Generic immunity standard Part 1 – Residential commercial, and light industry.”
  - EN 61000-4-2 – 1995, A1:1998, A2 – 2001 – “Electrostatic Discharge Immunity Test”
  - EN 61000-4-3 – 2002 – “Radiated, Radio-Frequency, Electromagnetic Field Immunity Test”
  - EN 61000-4-4 – 1995, A1:2001, A2:2001 – “Electrical Fast Transient/Burst Immunity Test”
  - EN 61000-4-5 – 1995, A1:2001 – “Surge Immunity Test”
  - EN 61000-4-6 – 1996, A1:2001 – “Immunity To Conducted Disturbances, Induced By Radio-Frequency Fields”
  - EN 61000-4-8 – 1993, A1:2001 – "Power Frequency Magnetic Field Immunity Test”
  - EN 61000-4-11 Second Edition – 2004 – “Voltage Dips, Short Interruptions And Voltage Variations Immunity Tests”
- EN 61000-3-2 – 2000 – “Limits For Harmonic Current Emissions (Equipment Input Current Less Than/Equal To 16 A Per Phase)” Class A
- EN 61000-3-3 – 1995, A1:2001 – “Limitation Of Voltage Fluctuations And Flicker In Low-Voltage Supply Systems For Equipment With Rated Current Less Than Or Equal To 16 A”

VCCI Class A Statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

Laser Safety Information

This product may use Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

Electrostatic Discharge Sensitivity (ESDS) Precautions

The assemblies used in the switch chassis are ESD sensitive. Observe ESD handling procedures when handling any assembly used in the switch chassis.

Accessible Parts

The following field replaceable units (FRUs) are supported by the SANbox 6142 router:

- Small form-factor pluggable (SFP) optical transceivers

License Agreements

Refer to the *QLogic Software End User License Agreement* for a complete listing of all license agreements affecting this product.

General Public License

QLogic SANbox routers are powered by the Linux operating system. A machine-readable copy of the Linux source code is available upon written request to the following address. A nominal fee will be charged for reproduction, shipping, and handling costs in accordance with the General Public License.

QLogic Corporation

26600 Aliso Viejo Parkway
Aliso Viejo, CA 92656
Attention – Technical Support – Source Request

CAUTION!

Installation of software or files not authorized by QLogic will immediately and irrevocably void all warranty and service contracts on the affected units.

The following General Public License has been reproduced with permission from:

GNU General Public License
Version 2, June 1991
Copyright 1989, 1991 Free Software Foundation, Inc.
59 Temple Place – Suite 330, Boston, MA 02111-1307, USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software - to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some Free Software Foundation software is covered by the GNU Library General Public License instead). You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new programs, and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author’s protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors’ reputation.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program propriety. To prevent this, we have made it clear that any patent must be licensed for everyone’s free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms And Conditions For Copying, Distribution and Modification

1. This license applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law – that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter,

translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License – they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if tis contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately public on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception – if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of the whole must be on the terms of this License, whose permissions for other Licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of paragraphs 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of paragraphs 1 and 2 above on a medium customarily used for software interchange – or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of paragraphs 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with paragraph b.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original Licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties of this License.

8. If, as a consequence of a court judgement or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyright interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

11. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

12. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of the software generally.

NO WARRANTY

13. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

14. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING

ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and an idea of what it does.

`Copyright (C) yyyy name of author`

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

You should have received a copy of the GNU General Public License along with this program; if not write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Also information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

`Gnomovision version 69, Copyright (C) year name of author`

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'. This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should the appropriate pats of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items - whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

`signature of Ty Coon, 1 April 1989`

`Ty Coon, President of Vice`

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

Availability

QLogic Technical Support for products under warranty is available during local standard working hours excluding QLogic Observed Holidays.

Training

QLogic offers certification training for the technical professional for both the SANblade® HBAs and the SANbox® switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com.

Contact Information

Support Headquarters	QLogic Corporation 12984 Valley View Road Eden Prairie, MN 55344-3657 USA
QLogic Web Site	www.qlogic.com
Technical Support Web Site	support.qlogic.com
Technical Support Email	support@qlogic.com
Technical Training Email	tech.training@qlogic.com

North American Region	
Email	support@qlogic.com
Phone	+1-952-932-4040
Fax	+1 952-974-4910
Europe, Middle East, and Africa Region	
Email	emeasupport@qlogic.com
Phone Numbers by Language	+353 1 6924960 - English +353 1 6924961 - Français +353 1 6924962 - Deutsch +353 1 6924963 - Español +353 1 6924964 - Português +353 1 6924965 - Italiano
Asia Pacific Region	
Email	apacsupport@qlogic.com
Phone Numbers by Language	+63-2-885-6712 - English +63-2-885-6713 - (Mandarin) +63-2-885-6714 - (Japanese) +63-2-885-6715 - (Korean)
Latin and South America Region	
Email	calasupport@qlogic.com
Phone Numbers by Language	+52 55 5278 7016 - English +52 55 5278 7017 - Español +52 55 5278 7015 - Português

2 General Description

This section describes the following features and capabilities of the SANbox 6142 router:

- Router Capabilities (see page 2-2)
- Licensed Features (see page 2-2)
- Remote SAN Island Connectivity (see page 2-4)
- Local SAN Island Connectivity (see page 2-6)
- FCIP - Fibre Channel over IP (see page 2-6)
- Chassis LEDs (see page 2-7)
- Chassis Controls (see page 2-8)
- Fibre Channel Ports (see page 2-10)
- Fibre Channel SFP Transceivers (see page 2-11)
- iSCSI/Gigabit Ethernet Port LEDs (see page 2-12)
- Ethernet Port – Management (see page 2-12)
- Serial Port see page 2-13)

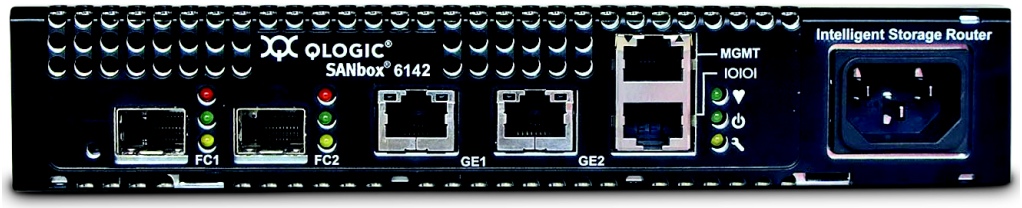


Figure 2-1 SANbox 6142 Router

Router Capabilities

The SANbox 6142 is a bi-directional FC-to-iSCSI router. It supports the following topologies:

- Two remote SAN islands (single or multi-vendor fabrics) (see page 2-4)
- Local connectivity (see page 2-6)
  - FC SAN islands (single or multi-vendor fabrics)
  - iSCSI Servers to FC SAN
  - FC servers to iSCSI SAN
- FCIP – Fibre Channel over IP (see page 2-6)

When using the SANbox 6142 to connect two Fibre Channel SANs, E-ports are not required on the Fiber Channel switches. This allows you to connect multi-vendor FC SANs (switches) without concern for the compatibility of the E-Ports and/or B-Ports between different switch vendors.

The SANbox 6142 has the following optional features:

- SmartWrite™ – Provides write performance improvements.
- Additional Server/Ports – Provides additional connectivity (see page 2-3).

Licensed Features

The SANbox 6142 router has two features that are available by a license key:

- SmartWrite
- Additional Server/Ports

SmartWrite

When connecting SAN over long distances, round-trip delays create significant impact to the performance. Typically, data writes involve two or more round-trip latencies that create a significant barrier to the data replication performance.

SmartWrite technology is designed to minimize the round-trip latency of any write I/O to a single round-trip latency.

This Feature Key offers the following benefits:

- Minimizes round-trip delays for any data write operation to a single round-trip latency.
- Allows load balancing over multiple IP links.

- Provides failover and failback between two gigabit ethernet links.
- Allows data compression. This is very useful when data round-trip latencies between two routers exceed more than 50 ms or long distance link rate is equal or less than 4500 Mbits/sec (DS-3 line rate)

SmartWrite is an optional feature which requires the purchase of a license key.

You may enter the **SmartWrite** feature key using the SANsurfer Router Manager (see page 7-19) or Command Line Interface (CLI) (see page A-41).

Qualified applications using SmartWrite include:

- Server connected to Remote FC Storage array
- Array Data Replication applications
  - EMC – Mirroview™ - EMC
  - EMC – SAN Copy™
  - HDS / Hitachi – True Copy™ with Fabric connect
  - HP – CA for XP

All other Data replication applications like IBM Shadow Copy™, EMC - SRDF, etc. should use the router's FCIP mode.

Additional Server/Ports

SANbox 6142 supports mapping of up to 62 Server/Ports between two SANs. The default configuration allows the mapping of 16 server/ports between SANs. For example, you may map 8 iSCSI initiators to FC SAN and map 8 FC devices from one FC SAN to another FC SAN. If your network requires more mappings, you can add a feature key to support additional mappings in 23 server/port increments as follows:

- 16 Server/Port mappings - the default configuration.
- 39 Server/Port mappings - includes the default 16 plus one "23 server/port license".
- 62 Server/Port mappings - includes the default 16 plus two "23 server/port licenses".

Additional Server/Ports is an optional feature which requires purchasing a license key. You may purchase up to two feature keys.

You can enter the Additional Server/Ports feature key using the SANsurfer Router Manager (see page 7-19) or Command Line Interface (CLI) (see page A-41).

Remote SAN Island Connectivity

The SANbox 6142 Intelligent Router supports inter-connecting remote SAN islands (see Figure 2-2).

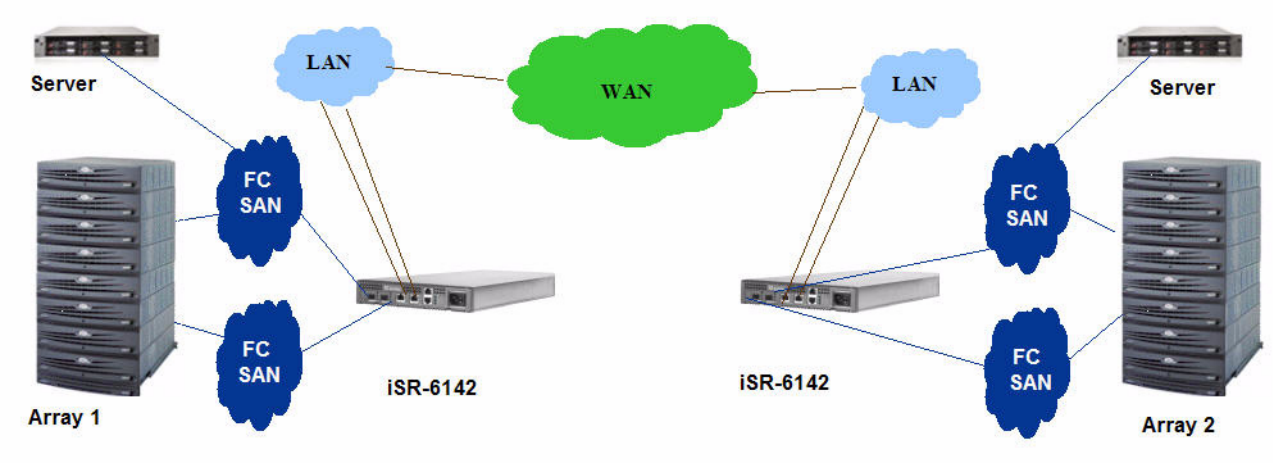


Figure 2-2 Remote SAN Island Connectivity

This configuration has the following additional requirements:

- At least one FC Port of SANbox 6142 connected to FC SAN.
- Accessibility between the iSCSI/ GE (GE identifies Gigabit Ethernet ports on the router) Port IP addresses of remote router and iSCSI/GE port IP addresses of local routers.
- Accessibility between the remote SANbox 6142 management port IP address and local SANbox 6142 management port IP address.

When connecting SANs over long distances, it's important to determine the round-trip latencies between two router connections. You can discover these round-trip latencies using the `ping` command in CLI. (See page A-25.)

Using this round-trip latency number, you can determine the window scaling factor for GE (iSCSI) port, as described in Performance Tuning on page 3-3. By default, window scaling is set to 1 (64K) TCP window size.

To map remote FC devices to local SAN:

1. If the remote router is not already associated with a local router, use either the SANsurfer Add Remote Router wizard (see page 7-68) or the CLI command `remotepeer add` (see page A-32) to associate the two routers with each other.
2. Use the SANsurfer Map Remote Initiator/Target wizard (see page 7-75) or the CLI `remotemap add` command (see page A-28) to create the initiator to target mapping.

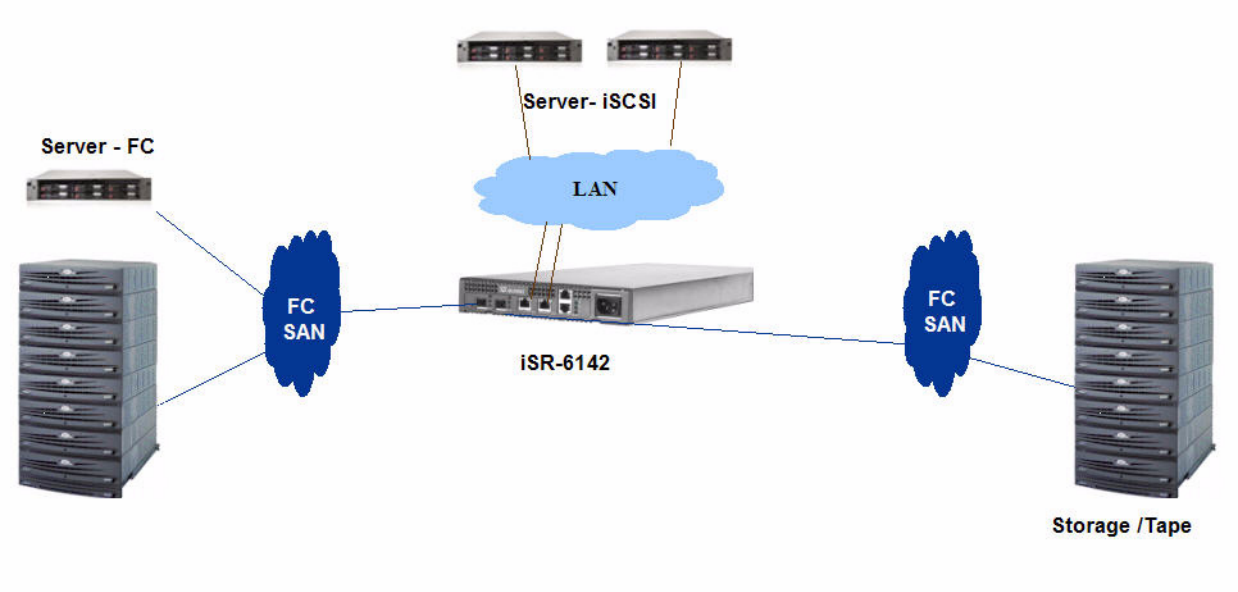


Figure 2-3 Local SAN Island Connectivity

The SANbox 6142 Intelligent Router supports inter-connecting local FC SAN islands. It also supports bridging iSCSI devices on the LAN to FC devices on the SAN (see Figure 2-33). It provides:

- FC storage from one SAN to a FC server on different SAN.
- FC storage to iSCSI servers.
- SCSI storage to FC servers.

Local SAN Island Connectivity

You can use either the SANsurfer Map Local Initiator/Target wizard (see page 7-55) or the CLI `localmap add` command (see page A-20) to map any of the following connections:

- iSCSI Server to an FC Device (Target)
- FC server to an iSCSI Device (Target)
- FC Server from one SAN to FC target on another SAN

CAUTION!

When adding multiple routers in the same physical SAN, you must import a given FC device from a remote SAN on only one SANbox 6142 in the local physical SAN. If you import the same FC device from multiple SANbox 6142s into the same physical SAN, the system duplicates FC world wide port names (WWPNs). This can disrupt the SAN.

FCIP - Fibre Channel over IP

The SANbox 6142 Intelligent Router supports FCIP, Fibre Channel over IP. The FCIP protocol as implemented in the router is not guaranteed nor has it been tested to be compatible with other vendor FCIP implementations. The router supports up to two FCIP routes; each route requires a dedicated FC and GE port pair.

- Merge FC fabrics over LAN/WAN
- N-port to fabric over LAN/WAN
- N-port to N-port over LAN/WAN

Chassis LEDs

The chassis LEDs shown in Figure 2-4 provide information about the router's operational status. These LEDs include the input power LED, heartbeat LED, and the system fault LED. To apply power to the router, plug the power cord into the router AC power receptacle and into a 100 VAC to 240 VAC, 50 Hz to 60 Hz power source.

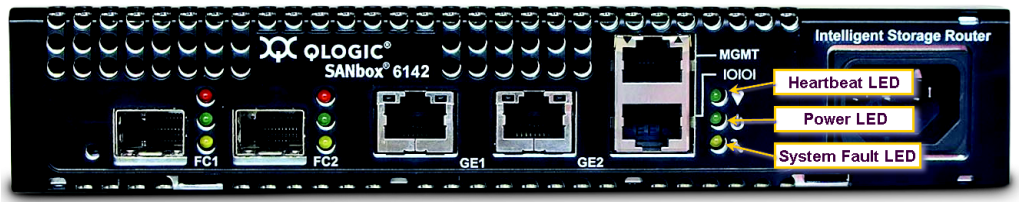


Figure 2-4 Chassis LEDs

Heartbeat LED (Green)

The heartbeat LED blinks once a second as long the the router firmware is operational.

Input Power LED (Green)

The power LED shows the voltage status at the router logic circuit board. During normal operation, this LED lights up to show that the router logic circuit board is receiving the DC voltage from the power supply.

System Fault LED (Amber)

The system fault LED lights up to show that a fault exists in the router firmware or hardware. Fault conditions include POST errors and over-temperature conditions. The LED shows a blink code for POST errors and the over temperature condition. See Figure 2-4 and Table 2-1.

Table 2-1. System Fault LED Blink Patterns

System Fault LED	Condition
OFF	OK (operational)
3 Blinks	System error
4 Blinks	Management port IP address conflict
5 Blinks	Over temperature
1 Blink	Beacon - synchronized with the Heartbeat LED

Chassis Controls

The maintenance button shown in Figure 2-5 is the only chassis control. Pressing this button resets the router or recovers the router if it has become disabled.

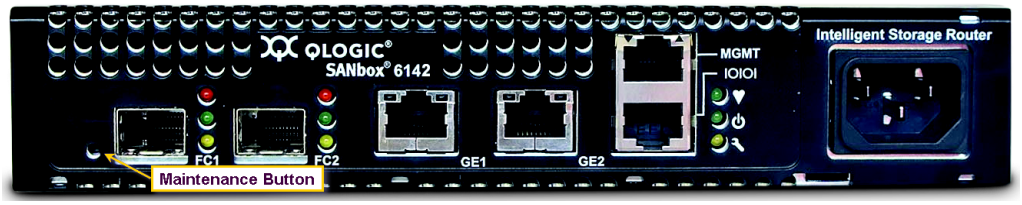


Figure 2-5 Chassis Controls

Maintenance Button

The maintenance button is a multifunction momentary switch on the front panel. It has the following functions:

- Reset a Router (see page 2-9)
- Reset and Select Boot Image (see page 2-9)
- Reset IP Address (see section page 2-9)
- Enable DHCP (see section page 2-9)
- Restore Factory Defaults (see page 2-9)

Reset a Router

To reset the router, use a pointed, nonmetallic tool to momentarily press and release (less than two seconds) the maintenance button. The router responds as follows:

1. All the chassis LEDs illuminate.
2. After about 2 seconds, the POST begins, turning off the heartbeat and system fault LEDs.
3. When the POST is complete, the power LED is on and the heartbeat LED flashes once per second.

Reset and Select Boot Image

You can reset the router using either the primary or secondary boot image:

- **Primary Image** – To reset the router and select the primary boot image, use a pointed, nonmetallic tool to press and hold the maintenance button until the heartbeat LED flashes once, then release the button. The router will boot from the primary boot image. The boot time is less than one minute.
- **Secondary Image** – To reset the router and select the secondary boot image, use a pointed, nonmetallic tool to press and hold the maintenance button until the heartbeat LED flashes twice, then release the button. The heartbeat LED flashes twice. The router boots from secondary boot image. The boot time is less than one minute.

Reset IP Address

To reset the router and restore the maintenance port IP address to the default (`10.0.0.1`), use a pointed, nonmetallic tool to press and hold the maintenance button until the heartbeat LED flashes six times, then release the button. The router boots and sets the maintenance port to IP address `10.0.0.1`. The boot time is less than one minute.

The IP address set by this method is not persistent; to make the change persistent, use the command line interface (CLI) or SANsurfer Router Manager to set the IP address. For more information, see page 7-4 and page A-3.

Enable DHCP

To reset the router and configure the maintenance port to use DHCP to acquire its IP address, use a pointed, nonmetallic tool to press and hold the maintenance button until the heartbeat LED flashes seven times, then release the button. The router boots and configures the maintenance port for DHCP. The boot time is less than one minute.

Enabling DHCP by this method is not persistent; to make the change persistent, use the command line interface (CLI) or SANsurfer Router Manager to enable DHCP. For details, see page 7-13 and page A-45.

Restore Factory Defaults

To reset the router and restore it to the factory default configuration, use a pointed, nonmetallic tool to press the maintenance button and hold it until the heartbeat LED flashes 20 times, then release the button. The router boots and is restored to the factory defaults. The boot time is less than one minute.

The router does the following when restored to the factory defaults:

- Resets all passwords.
- Resets the maintenance port IP address to 10.0.0.1.
- Disables the iSCSI ports and sets the IP address to 0.0.0.0.

- Erases all presentations.
- Erases all discovered initiators and targets.

Fibre Channel Ports

The SANbox 6142 router has two Fibre Channel ports, labeled FC1 and FC2, as shown in page 2-10.

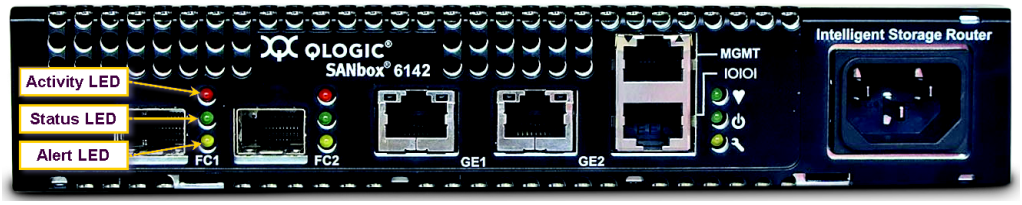


Figure 2-6 Fibre Channel LEDs

Each port is served by a small form-factor pluggable (SFP) optical transceiver and is capable of 1-Gbps or 2-Gbps transmission. SFPs are hot-pluggable. FC ports can self-discover both the connection type and transmission speed when connected to public devices or switches. The port LEDs are located to the right of their respective ports and provide status and activity information.

Fibre Channel Port LEDs

Each port has three LEDs:

- The amber LED (top) shows activity (data is passing through the port).
- The green LED (middle) shows the logged-in or initialization status of the connected devices. This LED flashes off to show the link rate, once for 1-Gbps speed, and twice for 2-Gbps speed.
- The yellow (bottom) LED shows an alert (port fault) condition.

Table 2-2 describes the LED blink patterns and their meanings.

Table 2-2. Port LEDs

Activity	Amber LED	Green LED	Yellow LED
Power OFF	OFF	OFF	OFF
Power ON (before firmware initialization)	ON	ON	ON

Table 2-2. Port LEDs

Activity	Amber LED	Green LED	Yellow LED
Online Link established at 1Gbit	OFF	3 seconds ON Flashes OFF once	OFF
Activity at 1 Gbps	ON	3 seconds ON Flashes OFF once	OFF
Online Link established at 2 Gbps	OFF	3 seconds ON Flashes OFF twice	OFF
Activity at 2 Gbps	ON	3 seconds ON Flashes OFF twice	OFF
Power ON (after firmware initialization and/or loss of synchronization)	OFF	ON	ON
Firmware error	OFF	OFF	ON

Fibre Channel SFP Transceivers

The SANbox 6142 router supports SFP optical transceivers for the Fibre Channel ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fibre optic cables plug into the transceivers, which then connect to the devices. The Fibre Channel ports are capable of transmitting at 1-Gbps or 2-Gbps; the transceiver must also be capable of delivering these rates.

The SFP transceivers are hot pluggable – you can remove or install a transceiver while the router is operating without harming the router or the transceiver. However, this interrupts communication with the connected device. For information about installing and removing SFP optical transceivers, see page 4-5.

iSCSI/Gigabit Ethernet Port LEDs

The iSCSI/gigabit Ethernet ports shown in Figure 2-7 are RJ-45 connectors that provide connection to an Ethernet SAN through a 10/100/1000 Base-T Ethernet cable. The ports are labeled GE1 and GE2.

These ports have two LEDs – the link status LED (green) and the activity LED (also green).

- The link status LED lights up continuously after the router establishes an Ethernet connection.
- The activity LED lights up when the router sends or receives data over the connection.

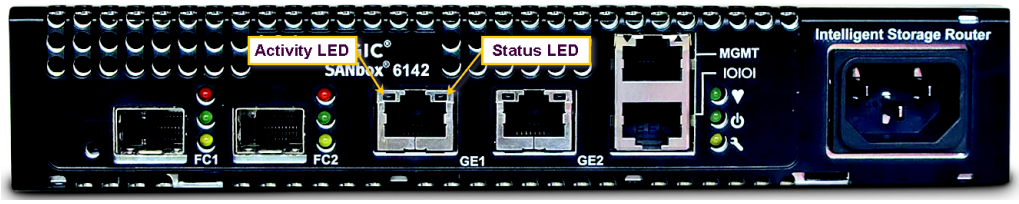


Figure 2-7 Gigabit Ethernet (iSCSI) Ports

Ethernet Port – Management

The Ethernet management port shown in Figure 2-8 is an RJ-45 connector that provides a connection to a management workstation through a 10/100 Base-T Ethernet cable. The port is labeled MGMT.

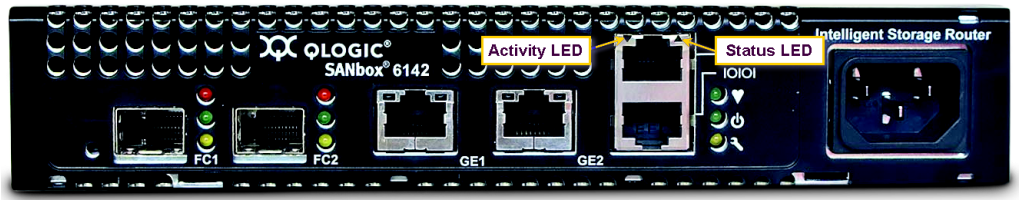


Figure 2-8 Ethernet Management Port

You can use a Windows®, Solaris™, or Linux™ workstation to configure and manage the router over an Ethernet connection using SANsurfer Router Manager, CLI, or simple network management protocol (SNMP).

The management Ethernet port has two LEDs:

- The link status LED (green) is on continuously after the router establishes an Ethernet connection.
- The activity LED (green) is on when the router sends or receives data over the Ethernet connection.

Serial Port

The SANbox 6142 router is equipped with an RS-232 serial port for maintenance purposes. Figure 2-9 shows the serial port location. It is labeled IOIOI. You can manage the router through the serial port using the CLI.

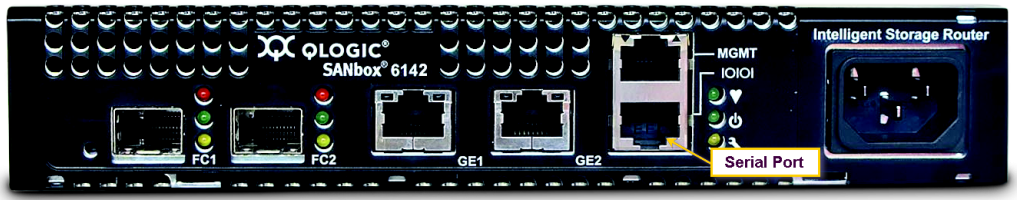


Figure 2-9 Serial Port

The serial port connection requires a standard, eight-wire Ethernet cable and the RJ45-to-DB9F adapter (supplied) to convert the Ethernet RJ45 connector to a female DB9 connector. Table 2-3 defines the serial port pins for the router's RJ45 connector. Table 2-4 defines the pinout for the RJ45 to DB9 adapter.

Table 2-3. Serial Port Pin Identification

RJ45 Pin Number	RJ-45 Pin Description
1	Clear to send (CTS)
2	Data set ready (DSR)
3	Receive data (RxD)
4	Signal ground (GND)
5	Data carrier detect (DCD)
6	Transmit data (TxD)
7	Data terminal ready (DTR)
8	Request to send (RTS)

Table 2-4. RJ-45 to DB-9 Adapter Pin Identification

RJ-45 Pin Number	DB-9F Pin Definition	DB-9 Pin Number	DB-9 Pin Definition
1	CTS	7	Request to send (RTS)
2	DSR	4	Data terminal ready (DTR)

Table 2-4. RJ-45 to DB-9 Adapter Pin Identification

RJ-45 Pin Number	DB-9F Pin Definition	DB-9 Pin Number	DB-9 Pin Definition
5	DCD		
3	RxD	3	Transmit data (TxD)
4	GND	5	Signal ground (GND)
6	TxD	2	Receive data (RxD)
7	DTR	1	Data carrier detect (DCD)
		6	Data set ready (DSR)
8	RTS	8	Clear to send (CTS)
		9	Ring indicator (RI)

3 Planning

This section describes how to plan for using the SANbox 6142 router. This includes the following considerations:

- Devices (see page 3-1)
- Device Access (see page 3-2)
- FC Performance (see page 3-2)
- iSCSI/Gigabit Ethernet Performance (see page 3-3)
- Performance Tuning (see page 3-3)
- Topology (see page 3-7)
- Fibre Channel Switch Ports and Zoning Requirements (see page 3-8)
- Multiple Routers (see page 3-8)
- Management (see page 3-8)
- Recovery (see page 3-8)
- Recovery (see page 3-8)
- Recovery (see page 3-9)
- Security (see page 3-9)

Devices

When planning to use the router, consider the number of devices and the anticipated demand. This will determine the required number of ports and in turn the number of routers.

The router uses SFP transceivers in the 1-Gbps/2-Gbps Fibre Channel (FC) ports, but some Fibre Channel (FC) devices may not use the same transceivers. Consider whether the FC device to be connected to the router uses SFP or gigabit interface converters (GBIC) transceivers, and choose fibre optic cables accordingly. Use LC-type cable connectors for small form-factor pluggable (SFP) transceivers and SC-type cable connectors for GBIC transceivers. Also consider the transmission speed compatibility of your devices, host bus adapters (HBAs), switches, and SFPs.

Device Access

Consider device access needs within the FC and iSCSI SANs. Access to an FC device is controlled by mapping FC device to specific iSCSI initiators. FC devices may be mapped to more than one initiator. Giving multiple initiators access to an FC device requires access management.

Fibre Channel

The Fibre Channel ports automatically discover all FC target devices, whether connected directly (loop) or by fabric (switch).

iSCSI

When an iSCSI initiator logs on, the router records the initiator's iSCSI name and IP address. The management interface (command line interface [CLI] or SANsurfer Router Manager) uses the initiator's information to simplify the mapping process.

FC Performance

The SANbox 6142 router supports Fibre Channel service at transmission rates of 1 Gbps or 2 Gbps with a maximum frame size of 2148 bytes. It supports Ethernet service at transmission rates of 1000-, 100- or 10-Mbps with a maximum transmission unit (MTU) size of 1500 or 9000 (jumbo frames). Related performance characteristics include the following:

- Distance (see page 3-2)
- Bandwidth (see page 3-3)
- Latency (see page 3-3)

Distance

Consider the physical distance between Fibre Channel devices. Choose SFP transceivers that are compatible with the cable type and distance you need.

Each Fibre Channel port is supported by a data buffer with a three-credit capacity; that is, three maximum sized frames. For fibre optic cables, this enables full bandwidth over the following approximate distances:

- 5 kilometers at 1 Gbps (0.6 credits/Km)
- 2.5 kilometers at 2 Gbps (1.2 credits/Km)

Transmitting data beyond these distances reduces efficiency because the transmitting port must wait for an acknowledgement before sending the next frame.

Bandwidth

Bandwidth measures the amount of data transmitted over a channel or network. A 1-Gbps/2-Gbps FC port can transmit or receive at nominal rates of 1- or 2-Gbps, depending on the device to which it is connected. This corresponds to actual bandwidth values of 106 MB and 212 MB, respectively. WAN data rates range from 1.5 megabits per second (T1) to greater than 600 megabits per second (OC-12)

Latency

Latency measures how long a transaction takes to travel through the router or over a communication link.

iSCSI/Gigabit Ethernet Performance

The SANbox 6142 router supports Ethernet service at transmission rates of 1000-, 100- or 10-Mbps with a MTU size of 1500 or 9000 (jumbo frames). Related performance characteristics include the following:

- Distance
- Bandwidth
- Latency

Distance

Consider the physical distance between routers. This is usually measured in round-trip delay. Round-trip delay ranges anywhere from less than 1 millisecond to as great as 250 milliseconds.

Performance Tuning

Properly configuring the router maximizes its performance. Knowing the round-trip delay (distance) between routers and the WAN effective data rate (connection type) allows the routers to be tuned for optimal performance. The following tables provide TCP Window Scaling Factor and Window Size settings for specific WAN environments. A table is provided for each connection type.

Table 3-1. T1 / DS-1 – 1.554 Mbits/Sec

Round Trip delay (ms)	Total Window Size (bytes)	Scaling Factor
250	64 K	1
100	32 K	0
50	32 K	0

Table 3-1. T1 / DS-1 – 1.554 Mbits/Sec

Round Trip delay (ms)	Total Window Size (bytes)	Scaling Factor
25	32 K	0
20	32 K	0
15	32 K	0
10	32 K	0
5	32 K	0
2.5	32 K	0
1 or less	32 K	0

Table 3-2. T3 / DS-3 – 45 Mbits/Sec

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
250	1 MB	5
100	512 K	4
50	256 K	3
25	128 K	2
20	128 K	2
15	64-128 K	1 or 2
10	64 K	1
5	32 K	0
2.5	32 K	0
1 or less	32 K	0

Table 3-3. DS-5 – 400 Mbits/Sec

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
250	1 MB	5
100	1 MB	5

Table 3-3. DS-5 – 400 Mbits/Sec (Continued)

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
50	1 MB	5
25	1 MB	5
20	1 MB	5
15	1 MB	5
10	512 K	4
5	256 K	3
2.5	128 K	2
1 or less	64 K	1

Table 3-4. OC-1 – 50 Mbits/Sec

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
250	1 MB	5
100	512 K	4
50	256 K	3
25	128 K	2
20	128 K	2
15	64-128 K	1 or 2
10	64 K	1
5	32 K	0
2.5	32 K	0
1 or less	32 K	0

Table 3-5. OC-3 – 150 Mbits/Sec

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
250	1 MB	5
100	1 MB	5
50	1 MB	5
25	512 K	4
20	512 K	4
15	256 K	3
10	256 K	3
5	128 K	2
2.5	64 K	1
1 or less	32 K	0

Table 3-6. OC-12 and Above – 621 Mbits/Sec

Round Trip Delay (ms)	Total Window Size (bytes)	Scaling Factor
250	1 MB	5
100	1 MB	5
50	1 MB	5
25	1 MB	5
20	1 MB	5
15	1 MB	5
10	1 MB	5
5	512 K	4
2.5	256 K	3
1 or less	64 K	1

Topology

The SANbox 6142 supports two distinct topologies: interconnecting local SANs (see Figure 3-1) and interconnecting remote SANs (see Figure 3-2).

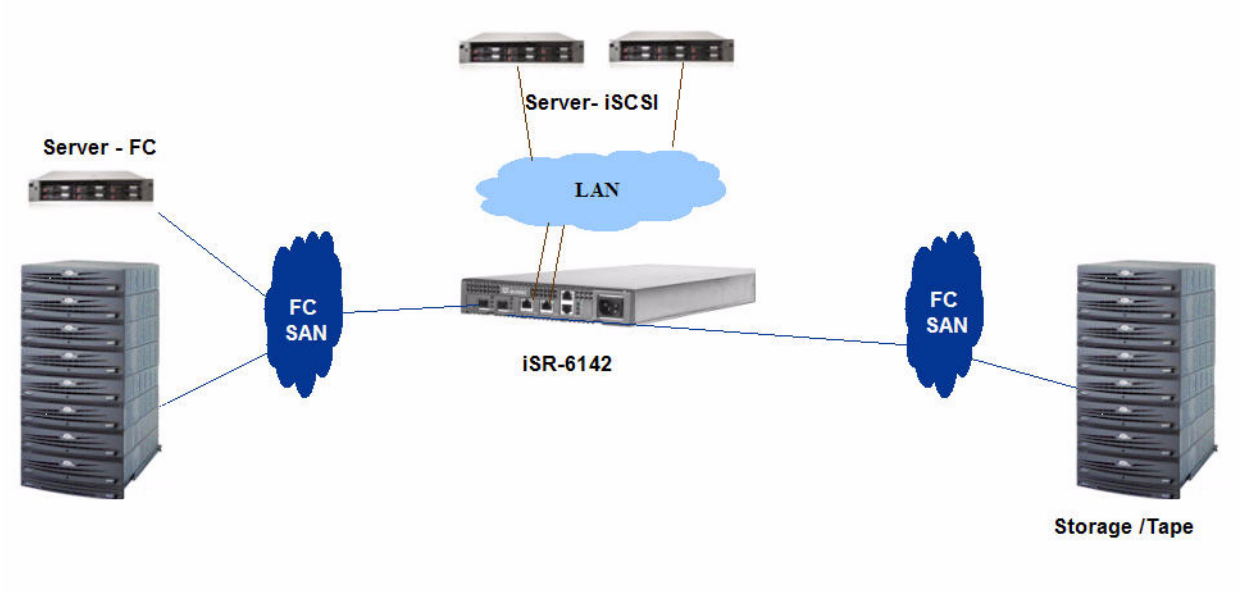


Figure 3-1 LAN Topology - Local SAN Interconnect

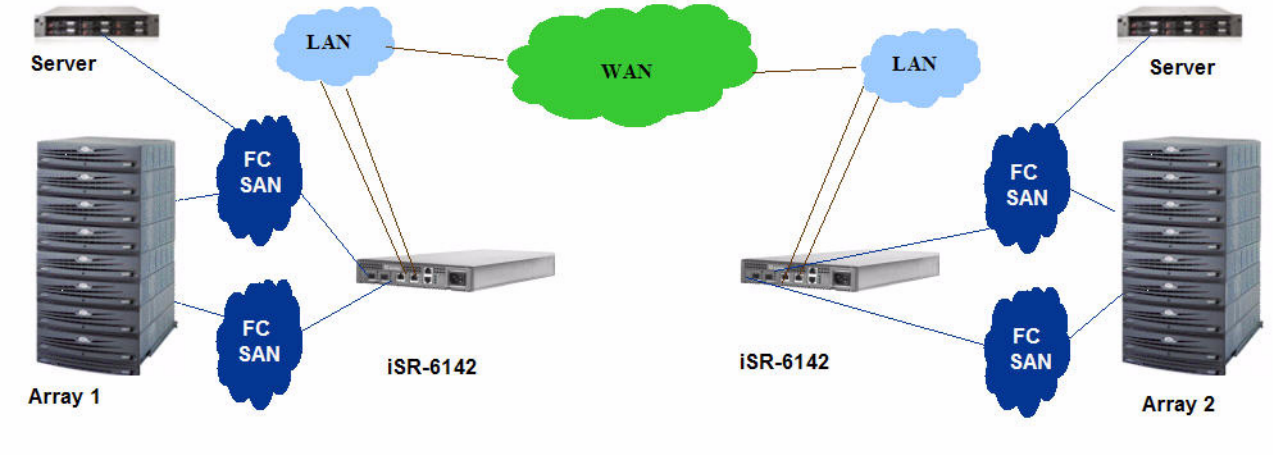


Figure 3-2 WAN Topology - Remote SAN Interconnect

Fibre Channel Switch Ports and Zoning Requirements

The SANbox 6142 FC ports are configured as loop ports. Therefore, the FC switch port, (where SANbox 6142 FC port is connected) must be configured to support a loop topology such as fibre loop port (FL-Port) or generic port (G-Port).

The SANbox 6142 uses its local FC ports for discovering local FC devices in the SAN.

We recommend that any FC switch connected to the SANbox 6142 use Fibre Channel World Wide Port name (WWPN) based zoning. This requires adding the router's FC world wide port names (WWPN) in all local switch zones and the remote router's FC WWPNs in all remote switch zones.

Multiple Routers

By connecting multiple routers between your Fibre Channel SANs and iSCSI SANs, you can eliminate any router as a single point of failure.

Management

The SANsurfer Router Manager application and CLI execute on a management workstation that enables you to configure, control, and maintain the router. Support platforms include Windows, Solaris, and Linux.

The router supports the following management interfaces:

- **SANsurfer Router Manager** – Graphical user interface application, which executes on a management workstation (see Section 7)
- Command line interface (**CLI)** – Executes on the router and is accessed via telnet or the serial port (see Appendix A)
- **SNMP** – Provides router status, traps, and alerts (see Appendix D)

Recovery

It is prudent to have a recovery process in case a router fails. Consider the following when developing a router recovery process:

- Save all firmware image files (updates) in a safe, well-know place, because you may:
  - Want to revert to a previous firmware version
  - Need the firmware image when replacing a router
  - Need the firmware image when adding a router to your site

- Save the router's configuration (as a new file) after every configuration change, because you may:
  - Want to revert to a previous configuration
  - Need to configure a replacement router
- Save the router's mappings (as a new file) after every mapping change, because you may:
  - Want to revert to a previous mapping
  - Need to map a replacement router
  - Want to duplicate the mapping on a second router (for backup)

Services

You can configure your router to suit the demands of your environment using a variety of router services. Familiarize yourself with the following router services and determine which ones you need:

- **Telnet** – Enables router management over a telnet connection.
- **Router management** – Provides for out-of-band router management using the SANsurfer Router Manager.
- **Simple network management protocol (SNMP)** – Provides monitoring of the router using third-party applications that use SNMP.
- **Network time protocol (NTP)** – Provides for synchronizing the router and the workstation dates and times with an NTP server. NTP is disabled (and not configured) by default.
- **File transfer protocol (FTP)** – Provides for transferring files rapidly between the workstation and router using FTP.

Security

Passwords provide router security. The SANsurfer Router Manager uses a default password. Once connected, the SANsurfer Router Manager prompts for a password whenever a user attempts to change a setting.

The CLI interface requires a username and password to start. CLI must be in an admin session to perform any set operations. An admin session requires a password.

Once logged on, you can change the password using the application's security features.

Notes

4 Installation

This section describes how to install and configure a SANbox 6142 router. It also includes firmware installation instructions. This includes the following topics:

- Site Requirements (this page)
- SANbox 6142 Router Installation (see page 4-2)
- Firmware Installation (see page 4-11)

Site Requirements

The requirements in the following sections must be met when installing a SANbox 6142 router:

- Management Workstation (this page)
- Power Requirements (see page 4-2)
- Environmental Conditions (see page 4-2)

Management Workstation

The management workstation running the SANsurfer iSCSI/FC Router Manager must meet the requirements listed in Table 4-1.

Table 4-1. Management Workstation Requirements

Item	Description
Operating system	One of the following: ■ Windows® 2000/2003/XP ■ Solaris 8/9/10 ■ Linux® Red Hat EL 3.x ■ SuSE® Linux 9.0 Enterprise ■ Mac OS® X 10.3
Memory	256 MB or more
Disk space	150 MB per installation

Table 4-1. Management Workstation Requirements

Item	Description
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet browser	One of the following: ■ Microsoft Internet Explorer 5.0 and later ■ Netscape Navigator® 4.72 and later ■ Mozilla® 1.02 and later ■ Safari™ ■ Java 2 runtime environment to support the web applet

Power Requirements

Power requirements for the SANbox 6142 router are 0.5 Amps at 100-125 VAC, 50 Hz to 60 Hz or 0.25 Amps at 200-240 VAC, 50 Hz to 60 Hz.

Environmental Conditions

Consider the factors that affect the climate in your facility, such as equipment heat dissipation and ventilation. The router requires the following operating conditions:

- Operating temperature range – 5–40°C (41–104°F)
- Relative humidity – 15–90 percent, non-condensing

SANbox 6142 Router Installation

Prior to installing the router, unpack the router and accessories. The SANbox 6142 router is shipped with the following components, shown in Figure 4-1:

- Power cord.
- Adapter (RJ45 to DB9F) for connecting the router's serial port to a workstation used for configuring and managing the router. A standard Cat5 Ethernet cable is required (not supplied) to connect the adapter to the router. The adapter connects directly to the workstation's serial (COM) port.

Figure 4-1 SANbox 6142 Router and Accessories

To install the SANbox 6142 router:

1. Complete the pre-installation checklist (see page 4-4).
2. Mount the router (see page 4-4).
3. Install the transceivers (see page 4-5).
4. Connect the management workstation to the router (see page 4-5).
5. Configure the management workstation (see page 4-5).
6. Install the management application (see page 4-7).
7. Start the management application (see page 4-8).
8. Connect the router to AC power (see page 4-9).
9. Configure the router (see page 4-10).
10. Cable FC and iSCSI devices to the router (see page 4-11).

Pre-installation Check List

During the initial configuration process, the system prompts you for the parameters listed in Table 4-2. Fill out the table before installation to expedite the configuration process.

Table 4-2. Pre-installation Checklist

Symbolic name of this router	
Management port IP address (if not using DHCP)	
Management port subnet mask (if not using DHCP)	
Management port gateway IP address (if not using DHCP)	
iSCSI Port 1 (GE-1) IP address	
iSCSI Port 1 (GE-1) subnet mask	
iSCSI Port 1 (GE-1) gateway IP address	
iSCSI Port 1 (GE-1) iSNS[a] IP address	
iSCSI Port 2 (GE-2) IP address	
iSCSI Port 2 (GE-2) subnet mask	
iSCSI Port 2 (GE-2) gateway IP address	
iSCSI Port 2 (GE-2) iSNS IP address	

[a] Internet Storage Name Service

Mount the Router

You can place the router on a flat surface or mount it in a standard 19-inch Electronic Industries Association (EIA) rack. See the product specification for weight and dimensions. Rack mounting requires a QLogic rack mounting kit (Part No. ISR614X-RACKKIT). Contact QLogic for more information.

If you mount the router in a closed or multi-unit rack assembly, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature for the router.

Install the Transceivers

The router supports a variety of SFP transceivers. To install a transceiver, insert the transceiver into the port and gently press until it snaps in place. To remove a transceiver, gently press the transceiver into the port to release tension, then pull the release tab or lever and remove the transceiver. Different transceiver manufactures have different release mechanisms. Consult the documentation of your transceiver.

NOTE:

The transceiver fits only one way. If the transceiver does not install under gentle pressure, flip it over and try again.

Connect the Management Workstation to the Router

You can manage the router using the SANsurfer iSCSI/FC Router Manager or the command line interface (CLI). SANsurfer iSCSI/FC Router Manager requires an Ethernet connection to the router. The CLI can use an Ethernet connection or a serial connection. Choose the router management method, then connect the management workstation to the router in one of the following ways:

- Indirect Ethernet connection from the management workstation to the router RJ-45 connector through an Ethernet switch or hub. This requires a 10/100 Base-T straight-through cable.
- Direct Ethernet connection from the management workstation to the router RJ-45 Ethernet connector. This requires a 10/100 Base-T crossover cable.
- Serial port connection from the management workstation to the router RS-232 serial port connector. This requires a 10/100 Base-T straight-through cable and an RJ45-to-DB9F adapter (included with the router).

Configure the Management Workstation

The router comes from the factory with a default IP address (10.0.0.1). Prior to product installation, follow the procedures based on your configuration method:

- If you plan to configure the router through the management Ethernet port (using the SANsurfer GUI or CLI via telnet), you must initially configure the workstation as described in Setting the Workstation IP Address on page 4-6.
- If you plan to configure the router using the management COM port, configure the workstation as described in Configuring the Workstation Serial Port on page 4-6.

Setting the Workstation IP Address

The IP address of a new router is `10.0.0.1`. To ensure that your workstation is configured to communicate with the `10.0.0` subnet, refer to the following instructions for your workstation:

- Steps for different versions of Windows vary. For a Windows 2000 workstation, do the following:
  a. From the Windows **Start** menu, select **Settings>Control Panel>Network and Dial-up Connections**.
  b. Click **Make New Connection**.
  c. Click **Connect to a private network through the Internet**, then click **Next**.
  d. Enter `10.0.0.253` for the IP address.
- For different versions of Windows, consult the Windows Help files.
- For Linux or Solaris workstation, open a command window and enter the following command, where `<interface>` is your interface name:
  `ifconfig <interface> ipaddress 10.0.0.253 netmask 255.255.255.0 up`

Configuring the Workstation Serial Port

To configure the workstation serial port:

1. Connect the cable with RJ45 to DB9F adapter from a COM port on the management workstation to the serial port on the router.
2. Configure the workstation serial port according to your platform. These steps may vary according to the version of Windows you use:
   - For Windows:
     a. Open the HyperTerminal application. From the Windows Start menu, select **Programs>Accessories>HyperTerminal>HyperTerminal**.
     b. Enter a name for the router connection, choose an icon in the Connection Description window, then click **OK**.
     c. Enter the following COM Port settings in the COM Properties window and click **OK**.
     Bits per second – 115200
     Data Bits – 8
     Parity – None
     Stop Bits – 1
     Flow Control – None

- For Linux:

  a. Set up minicom to use the serial port. Create or modify the `/etc/minirs.dfl` file with the following content:
  ```
  pr portdev/ttyS0
  pu minit
  pu mreset
  pu mhangup
  ```
  `pr portdev/ttyS0` specifies port 0 on the workstation. Choose the pr setting to match the workstation port to which you connected the router.

  b. Verify that all users have permission to run minicom. Review the `/etc/minicom.users` file and confirm that the line ALL exists or that there are specific user entries.

- For Solaris – Modify the `/etc/remote` file to include the following lines. `/dev/term/a` refers to serial port a. Choose the "`dv`" setting to match the workstation port to which you connected the router.
  SANbox:
  ```
  \:dv=/dev/term/a:br#115200:el=^C^S^Q^U^D:ie=%$:oe=^
  D:
  ```

3. Connect the router to the power (see page 4-9).

Install SANsurfer iSCSI/FC Router Manager

You can manage the router using the SANsurfer iSCSI/FC Router Manager application. The following sections describe how to install the application on either a Windows or Linux workstation. See Section 7 for information on how to use SANsurfer iSCSI/FC Router Manager.

Windows Installation

Perform the following steps to install the SANsurfer iSCSI/FC Router Manager application from the QLogic website to a PC workstation:

1. Close all programs currently running.
2. Go to the QLogic download site:
   http://support.qlogic.com/support/drivers_software.aspx
3. Select the **Intelligent Storage Routers** icon.
4. Select **SANbox 6142** in the product selection window and click **Go**.
5. Under the product name column, select the link to the SANsurfer Router Manager for your operating system.
6. Read the license agreement and click **Agree**.
7. Follow the system prompts to uncompress and install the application.

Linux Installation

Perform the following steps to install the SANsurfer iSCSI/FC Router Manager application from the QLogic website to a Linux workstation:

1. Go to the QLogic download site: http://support.qlogic.com/support/drivers_software.aspx
2. Select the **Intelligent Storage Routers** icon.
3. Select **SANbox 6142** in the product selection window and click **Go**.
4. Under the product name column, select the link to the SANsurfer Router Manager for your operating system.
5. Read the license agreement and click **Agree**.
6. Save the file to your local system.
7. Uncompress the downloaded file and execute the `Linux_x.xx.bin` install program.
8. Follow the installation instructions.

Start SANsurfer iSCSI/FC Router Manager

For Windows, double-click the SANsurfer iSCSI/FC Router Manager shortcut, or select SANsurfer **iSCSI/FC Router Manager** from the **Start** menu, depending on how you installed the SANsurfer iSCSI/FC Router Manager application. From a command line, you can enter the following command:

```
<install_directory>SANsurfer_Router_Manager.exe
```

For Linux, enter the following command:

```
<install_directory>./SANsurfer_Router_Manager
```

Connect the Router to AC Power

WARNING!!

This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the router chassis. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable must meet the following requirements:

- For 125 Volt electrical service – the cable must be rated at 10 Amps and be approved by UL and CSA.
- For 250 Volt electrical service – the cable must be rated at 10 Amps, meet requirements of H05VV-F, and be approved by VDE, SEMKO, and DEMKO.

To power up the router, connect the power cord to the power receptacle on the router chassis and to a grounded AC outlet. The router responds in the following sequence:

1. The chassis LEDs (input power, heartbeat, system fault) light up, then all port LEDs light up.
2. After a couple of seconds the heartbeat and system fault LEDs go off, while the input power LED stays on. The router is executing the POST.
3. The POST completes after about 45 seconds and the heartbeat LED starts flashing at a one second rate. If an error has occurred, the System Fault LED will blink a pattern that indicates the fault reason. For more information about error blink patterns, see page 5-3.

Configure the Router

You can configure the router using the SANsurfer iSCSI/FC Router Manager application or the command line interface (CLI).

The SANsurfer Router Manager provides a Configuration Wizard you can use to configure the GE ports. If either of the router's GE ports have not been configured (IP address is 0.0.0.0), the Configuration Wizard starts automatically when the SANsurfer first connects with the router. The system uses the information collected in Table 4-2.

To configure the router using the command line interface:

1. Open a command window according to the type of workstation and connection:
   - Ethernet (all platforms) – Open a telnet session with the default router IP address and log in to the router with the default account name and password (guest/password).
     ```
     telnet 10.0.0.1
     username – guest
     password – ********
     ```
   - Serial – On Windows, open the HyperTerminal application. The next few steps may vary according to the version of Windows you use.
     a. From the Windows **Start** menu, select **Programs>Accessories>HyperTerminal>HyperTerminal**.
     b. Select the connection you created earlier and click **OK**.
   - Serial – On Linux, open a command window and enter the following command:
     ```
     minicom
     ```
2. Open an admin session and enter the commands to setup both iSCSI ports and the management interface. See Appendix A for command descriptions.
   ```
   QRouter #> admin start
   Password  –  ******
   QRouter (admin) #> set mgmt
   ……
   QRouter (admin) #> set iscsi 1
   ……
   QRouter (admin) #> set iscsi 2
   ……
   ```

Cable Devices to the Router

Connect cables to the SFP transceivers and their corresponding devices. Devices can have small form-factor pluggable (SFP) or small form-factor (SFF) transceivers or gigabit interface converters (GBIC). Lucent (LC)-type duplex fiber optic cable connectors are designed for SFP transceivers, while Subscriber-connector (SC)-type connectors are designed for GBICs. Choose the fiber optic cable with the connector combination that matches the device you are connecting to the router.

Firmware Installation

The router comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the SANsurfer iSCSI/FC Router Manager application or the CLI to install new firmware.

WARNING!!

Installing new firmware disrupts the router connectivity since you must reboot the router to activate the new firmware. The reboot may result in the transfer of incorrect data between devices connected to the router. QLogic recommends that you suspend activity on the interfaces before activating the new firmware.

Using SANsurfer iSCSI/FC Router Manager to Install Firmware

To install firmware using the SANsurfer iSCSI/FC Router Manager:

1. Double-click the desired router in the topology display.
2. In the Firmware Upload window, click **Select** to browse for and select the firmware file you want to upload.
3. Click **Start** to begin the firmware load process. A message displays a warning that the router will be reset to activate the firmware.
4. Click **OK** to continue firmware installation or click the **Cancel** button to cancel the firmware installation.

Using the CLI to Install Firmware

To use the CLI to install the firmware, transfer the firmware image file from a workstation to the router. Then use the CLI image unpack command to install the new firmware image:

1. At the workstation prompt, use the ftp command to go to the location on the router where you want to transfer the firmware image. For example:
```
C:\fwImage>ftp 172.17.137.190
Connected to 172.17.137.190.
220 (none) FTP server (GNU inetutils 1.4.2) ready.
```
2. Enter your username and password. For example:
```
User (172.17.137.190:(none)) - ftp
331 Guest login ok, type your name as password.
Password - ftp
230 Guest login ok, access restrictions apply.
```
3. At the ftp prompt, type `BIN` to set binary mode. For example:
```
ftp> bin
200 Type set to I.
```
4. Use the put command to transfer the firmware image file from the workstation to the router. For example:
```
ftp> put isr-6142-2_2_0_x.bin
200 PORT command successful.
150 Opening BINARY mode data connection for
'isr-6142-2_2_0_x.bin'.
226 Transfer complete.
ftp - 4822816 bytes sent in 0.41Seconds
11878.86Kbytes/sec.
```
5. Type `quit`. The firmware image has been transferred to the router.
6. Log on to the router as an `administrator`.
```
(none) login - guest
Password - password
*****************************************************
*                                                   *
*    QLogic Router Command Line Interface (QRCLI)   *
* *
*****************************************************
QRouter#> admin start
Password      - config
QRouter (admin) #>
```

7. Type the following command from the router, where x stands for the firmware image name:
   `image unpack isr-6142-2_2_0_x.bin`
   The following message displays:
   `Unpack Completed. Please reboot the system for FW to take affect.`
8. Type `reboot`. The following message displays:
   `Are you sure you want to reboot the System (y/n):`
9. Type `y` to reboot the system.

Notes

5 Diagnostics and Troubleshooting

Diagnostic information about the router is available through the chassis LEDs and the port LEDs. Diagnostic information is also available through the SANsurfer iSCSI/FC Router Manager and CLI event logs and error displays. This section provides the following diagnostic information:

- Chassis Diagnostics (this page)
- Power-On Self-Test Diagnostics (see page 5-2)
- LED Blink Patterns (see page 5-3)

This section also describes how to use maintenance mode to recover a disabled router (see page 5-5).

Chassis Diagnostics

The chassis LEDs show chassis diagnostics as shown in Figure 5-1.

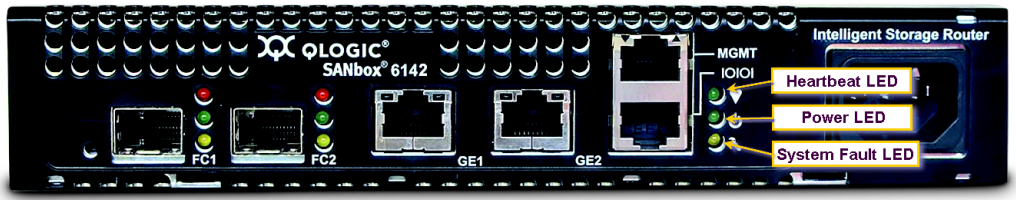


Figure 5-1 Chassis Diagnostic LEDs

This section describes the following conditions:

- Input Power LED is Off (see page 5-2)
- System Fault LED is On (see page 5-2)

Input Power LED is Off

The input power LED lights up to show that the router logic circuitry is receiving proper voltages. If the input power LED is off, do the following:

- Inspect power cord and connectors. Is the cord unplugged? Is the cord or connector damaged?
  - **Yes** – Make necessary corrections or repairs. If the condition remains, continue.
  - **No** – Continue.
- Inspect AC power source. Is the power source delivering the proper voltage?
  - **Yes** – Continue.
  - **No** – Make the necessary repairs. If the condition remains, continue.
- Replace the router.

System Fault LED is On

The System fault LED will blink a specific pattern to indicate the problem. If the system fault LED lights up, take necessary actions (see page 5-3).

Power-On Self-Test Diagnostics

The router performs a series of tests as part of its power-on procedure. The POST diagnostic program performs the following tests:

- Memory
- FLASH validation
- PCI device discovery
- Management Ethernet port

LED Blink Patterns

The Heartbeat and System Fault LEDs show the operational status of the router. When the POST completes with no errors, the heartbeat LED will blink once every second. When the router is in maintenance mode, the Heartbeat and System Fault LEDs are on continuously.

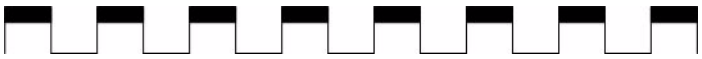
All other System Fault blink patterns show critical errors. The heartbeat LED shows an error blink pattern for the conditions listed in Table 5-1.

Table 5-1. System Fault LED Blink Patterns

System Fault LED	Condition
OFF	OK - Operational
3 Blinks, followed by pause	System error
4 Blinks, followed by pause	Management port IP address conflict
5 Blinks, followed by pause	Over temperature

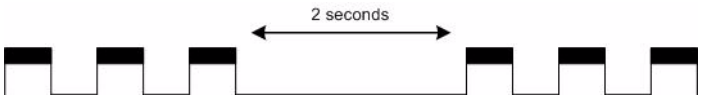
Heartbeat Blink Pattern

A blink pattern on the Heartbeat LED of one second ON followed by one second OFF means that the router is operating normally. The Heartbeat LED shows this pattern when the router firmware is operational.



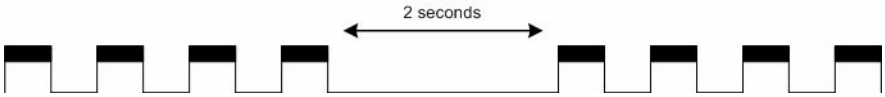
System Error Blink Pattern

The System Fault LED generates a three-blink pattern (once per second) followed by a two second pause to indicate a system error.



Management Port IP Address Conflict Blink Pattern

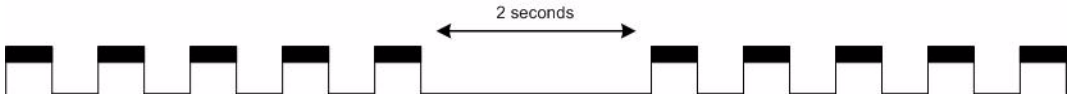
The System Fault LED generates a four-blink pattern (once per second) followed by a two second pause when the router detects an IP address conflict on the management Ethernet port.



You can clear the IP address conflict blinking using the CLI or SANsurfer Router Manager. Use the beacon OFF function.

Over-Temperature Blink Pattern

The System Fault LED generates a five-blink pattern (once per second) followed by a two second pause when the router is in an over-temperature condition. That is, the air temperature inside the router is over the failure temperature of 70°C (158°F).



If the system alert LED shows the over temperature blink pattern, do the following:

- Inspect the chassis air vents. Are the intake and exhaust vents clear?
  - **Yes** – Continue
  - **No** – Remove any debris from the fan intake and exhaust if necessary. If the condition remains, continue.
- Consider the ambient air temperature near the router and clearance around the router. Make necessary corrections. If the condition remains, open a command line window and log on to the router. Enter the Shutdown command, then power down the router. Contact your authorized maintenance provider.

Recovering a Router

You may have to recover a router for one of the following reasons:

- The password was changed and has been forgotten.
- The router's management IP address is unknown.

To recover the router's password, reset the password to the default by using the maintenance button (see page 2-8).

You can recover the router's IP address using either of the following methods:

- Connect to the serial console port (see page 2-13), then use the `CLI Set Mgmt` command reconfigure the management port (see page A-44).
- Use the maintenance button to reset the management port's IP to the factory default of `10.0.0.1` (see page 2-8).

Notes

6 Removal/Replacement

This section describes the removal and replacement procedures for the following field replaceable units (FRU):

- SFP transceivers
- The router (see page 6-2)

SFP Transceiver Removal and Replacement

You can remove and replace the SFP transceivers while the router is operating without damaging the router or the transceiver. However, doing so will interrupt transmission on the affected port until the transceiver is installed.

- To remove a transceiver, gently press the transceiver into the port to release the tension, then pull the release tab or lever and remove the transceiver. Different transceiver manufactures have different release mechanisms. Consult the documentation for your transceiver.
- To install a transceiver, insert the transceiver into the port and gently press until it snaps in place.

NOTE:

The SFP transceiver will fit only one way. If the SFP does not install under gentle pressure, flip it over and try again.

Router Removal and Replacement

Before you can remove and replace the router, you must turn off the power to the router and disconnect its power cable. The router will lose all the Fibre Channel and iSCSI connections.

Removal

To remove and replace a router, perform the following steps, as applicable:

1. Make sure all traffic (I/O operations to the router) subsides at the iSCSI initiator systems.
2. Save the configuration data of the router using the CLI FRU command (see page A-13).
3. Power down the router.
4. Disconnect the power cable.
5. Label all the cables so that they can be connected to the same ports on the replacement router.
6. Remove all the Fibre Channel and Ethernet cables.
7. Remove the router from the enclosure where it is mounted.

Replacement

Before replacing a router, you must first remove the previously installed router (as described above).

To install a replacement router:

1. Mount the router in the enclosure.
2. Reconnect the Fibre Channel and Ethernet cables to the ports where they were previously connected.
3. Connect the power cable to the router.
4. Using a management station, configure the management port IP address (see page 4-2).
5. Using a management workstation, restore the saved configuration or reconfigure the router as desired (see page A-13).

The replacement router should now be operational.

7 SANsurfer iSCSI/FC Router Manager

Introduction

The SANbox 6142 management application is a graphical user interface consisting of menus, buttons, and windows that you can use to manage SANbox 6142s from a workstation on Linux® and Windows® platforms. You can view and change network, port, security, and mapping configuration for one or more SANbox 6142s. The application displays the most current system information.

The SANsurfer iSCSI/FC Router Manager consists of a menu bar, a tool bar, a system tree, and information/status/data windows and tabs, as illustrated in Figure 7-1 and described in Table 7-1.

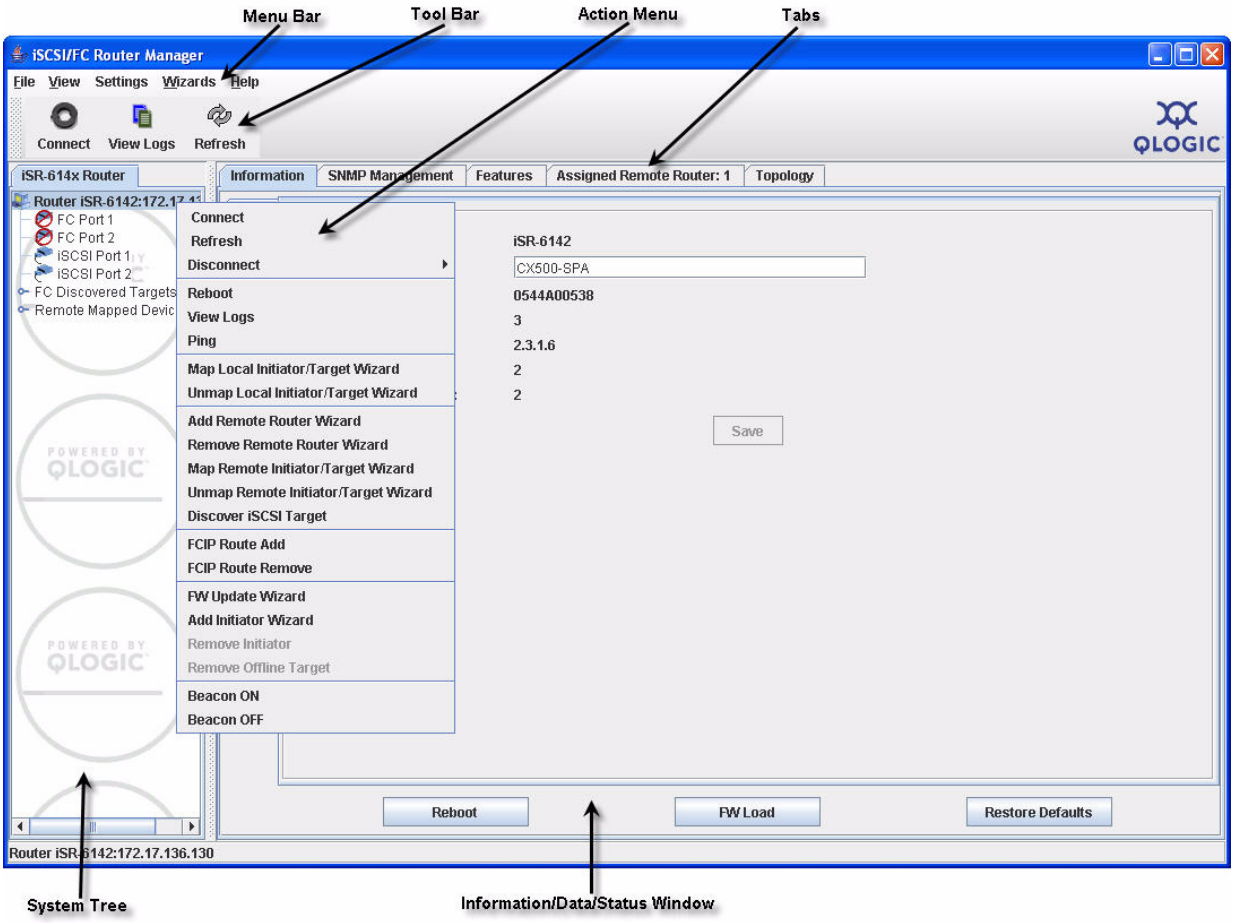


Figure 7-1 SANsurfer Router Manager Main Window

Table 7-1. SANsurfer Router Manager Main Window Sections

Item	Description
Menu Bar	The menu bar provides access to system functions and Wizards.
Tool Bar	The tool bar buttons provide quick access to the common application functions: **Connect**, **View Logs**, and **Refresh**.

Table 7-1. SANsurfer Router Manager Main Window Sections

Item	Description
System Tree	Located on the on the left side of the display, the system tree shows the connected systems and their components. An entry handle located to the left of an entry in the tree shows that you can expand that entry. Click an entry handle or double-click the entry to expand or collapse a system tree entry. Click and drag the window border to re-size the window.
Action Menu	Right-click anywhere on the system tree window to open the action menu. This menu provides a shortcut to actions available elsewhere in the SANsurfer Router Manager. If you select an initiator or target (highlighted), then right-click in the system tree, the action menu activates the **Remove Initiator** and **Remove Offline Target** selections.
Information, Configuration, and Status windows	These windows present the corresponding information, configuration, or status for the window tab you select. Some windows contain a scroll bar to browse the window contents.Click and drag the window border to re-size the window.
Window Tabs	The window tab determines what is displayed in the window.

Menu Bar

Figure 7-2 shows the menu bar options. The following sections describe them.

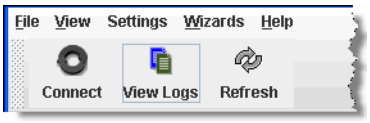


Figure 7-2 Menu Bar

File Menu

Figure 7-3 shows the **File** menu. The following paragraphs describe it.

Figure 7-3 File Menu

- **Save FRU** – Saves the router's configuration and persistent data to a file.
- **Restore FRU** – Restores the router's configuration and persistent data from a file.
- **Exit** – Exits the SANsurfer iSCSI/FC Router Manager.

View Menu

Figure 7-4 shows the **View** menu. The following paragraph describes it.

Figure 7-4 View Menu

- **View Logs** – Opens the window displaying the system logs.

Settings Menu

Figure 7-5 shows the **Settings** menu. The following paragraph describes it.

Figure 7-5 Settings Menu

- **Broadcast** – Opens the Broadcast Settings window, which allows you to configure the broadcast options. The workstation sends Broadcast messages to locate routers within the same IP subnet as the workstation running the SANsurfer Router Manager application. Figure 7-6 shows the Broadcast Settings dialog box. The following paragraphs describe its options.

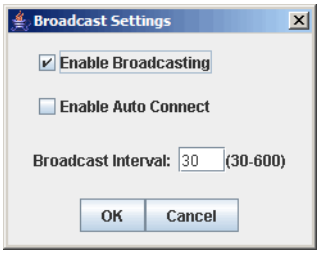


Figure 7-6 Broadcast Settings Menu

- **Enable Broadcast** – Enables broadcast messages sent to locate routers in the IP subnet.
- **Enable Auto Connect** – Enables the SANsurfer Router Manager to automatically connect with routers discovered by the broadcast.
- **Broadcast Interval** – Lets you enter the time interval at which the SANsurfer Router Manager sends broadcast messages to locate routers within the same IP subnet as the workstation.

Wizards Menu

Figure 7-7 shows the **Wizards** menu. The following paragraphs describe it.

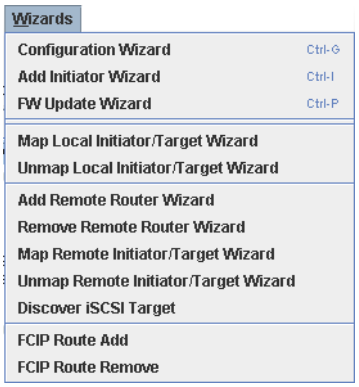


Figure 7-7 Wizards Menu

- **Configuration Wizard** – Launches the iSCSI Port Configuration wizard, which allows you to configure the IP address and other parameters for an iSCSI port (see page 7-44).
- **Add Initiator Wizard** – Launches the iSCSI Add Initiator wizard, which allows you to configure the IP address and other parameters for an iSCSI initiator (see page 7-49).
- **FW Update Wizard** – Launches the Firmware Update wizard, which allows you to update the SANbox 6142 router's firmware image. You can select the firmware image from a menu that allows browsing (see page 7-51).

- **Map Local Initiator/Target Wizard** – Launches the Map Local wizard, which allows you to map a local initiator to a local target (see page 7-55).
- **Unmap Local Initiator/Target Wizard** – Launches the Unmap Local wizard, which allows you to delete a local initiator from a local target mapping (see page 7-63).
- **Add Remote Router Wizard** – Launches the Add Remote Router wizard, which allows you to assign local router to a remote router as peers (see page 7-68).
- **Remove Remote Router Wizard** – Launches the Remove Remote Router wizard, which allows you to remove a local-to-remote router peer assignment (see page 7-72).
- **Map Remote Initiator/Target Wizard** – Launches the Map Remote wizard, which allows you to map an initiator to a target device, one of which is on a remoter router (see page 7-75).
- **Unmap Remote Initiator/Target Wizard** – Launches the Unmap Remote wizard, which allows you to delete an initiator-to-target device mapping (see page 7-81).
- **Discover iSCSI Target** – Launches the Discover iSCSI Target wizard, which allows you to specify the IP address of the iSCSI Target to be discovered. The target is added to the discovered targets list (see section page 7-84).
- **FCIP Route Add** – Launches the (Fiber channel over IP) FCIP Route Add wizard, which allows you to select – the resources used for the route, the IP address of the remote FCIP peer, IP parameters, Virtual Lan (VLAN) support, compression and bandwidth limit (see page 7-86).
- **FCIP Route Remove** – Launches the FCIP Route Remove wizard, which allows you to remove an existing FCIP Route, freeing the resources (FC and GE ports) used by the route (see page 7-92).

Help Menu

Figure 7-8 shows the **Help** menu. The following paragraphs describe it.

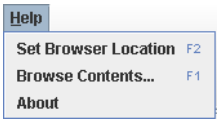


Figure 7-8 Help Menu

Set Browser Location – Allows you to specify the browser that launches when you view the online help for the SANsurfer iSCSI/FC Router Manager.

Browse Contents – Launches the online help for the SANsurfer iSCSI/FC Router Manager.

About – Displays the application version information.

Tool Bar

Figure 7-9 shows the tool bar. The following paragraphs describe it.

Figure 7-9 Tool Bar

The tool bar consists of a row of graphical buttons that allow you to perform common functions – connect, view log files, and refresh the current display. You can move the tool bar in the display by clicking and dragging the handle at the tool bar's left edge.

- **Connect** – Adds a SANbox 6142 router to the system tree view.
- **View Logs** – Opens a window to display the system log data.
- **Refresh** – Updates the display with current information.

Action Menu

The action menu provides short cuts to actions and wizards available elsewhere in the SANsurfer iSCSI/FC Router Manager. To open this menu, right-click anywhere within the router's node in the system tree window. Figure 7-10 illustrates the action menu and the following paragraphs describe each available option.

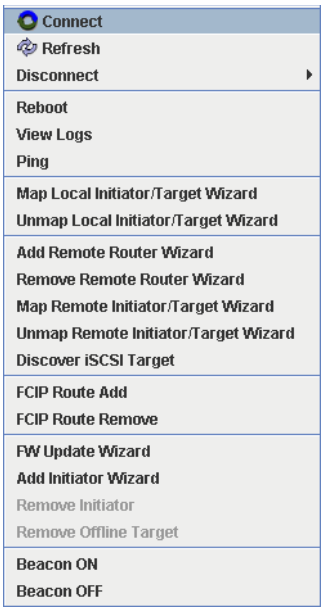


Figure 7-10 Action Menu

- **Connect** – Adds a **SANbox 6142** router to the system tree view.
- **Refresh** – Updates the display with current information.
- **Disconnect** – Disconnects from a **SANbox 6142** router, removing it from the system tree.
- **Reboot** – Reboots the SANbox 6142 router.
- **View Logs** – Opens the View Logs window.
- **Ping** – Initiates a ping from the specified port (management, GE1, or GE2) to a specified IP address.
- **Map Local Initiator/Target Wizard** – Launches the Map Local Initiator/Target Wizard, which allows you to map a local initiator to a local target (see page 7-55).
- **Unmap Local Initiator/Target Wizard** – Launches the Unmap Local Initiator/Target Wizard, which allows you to delete a local initiator from a local target mapping (see page 7-63.)

- **Add Remote Router Wizard** – Launches the Add Remote Router Wizard, which allows you to assign local router to a remote router as peers (see page 7-68).
- **Remove Remote Router Wizard** – Launches the Remove Remote Router Wizard, which allows you to remove a local-to-remote router peer assignment (see page 7-72).
- **Map Remote Initiator/Target Wizard** – Launches the Map Remote Initiator/Target Wizard, which allows you to map an initiator to a target device, one of which is on a remoter router (see page 7-75).
- **Unmap Remote Initiator/Target Wizard** – Launches the Remote Mapped Device, which allows you to delete an initiator-to-target device mapping (see page 7-81).
- **Discover iSCSI Target** – Launches the Discover iSCSI Target Wizard, which allows you to specify the IP address of the iSCSI Target to be discovered. The target is added to the discovered targets list (see page 7-84).
- **FCIP Route Add** – Launches the FCIP Route Add Wizard wizard, which allows you to select the resources used for the route, the IP address of the remote FCIP peer, IP parameters, VLAN support, compression and bandwidth limit (see page 7-86).
- **FCIP Route Remove** – Launches the FCIP Route Remove Wizard wizard, which allows you to remove an existing FCIP Route freeing the resources (FC and GE ports) used by the route. (See page 7-92).
- **FW Update Wizard** – Launches the FW Update Wizard, which allows you to update the router's firmware (see page 7-51).
- **Add Initiator Wizard** – Launches the Add Initiator Wizard, which allows you to enter an iSCSI initiator into the system database (see page 7-49).
- **Remove Initiator** – Removes the selected iSCSI initiator. This option is available only when an initiator is selected (highlighted) in the system tree.
- **Remove Offline Target** – Removes the selected offline Fibre Channel target. This option is available only when an offline FC target is selected (highlighted) in the system tree.
- **Beacon ON** – Turns on the **SANbox 6142** router beacon to locate the router quickly.
- **Beacon OFF** – Turns off the **SANbox 6142** router beacon.

System Tree Window

Figure 7-11 shows the system tree window. The following sections described it.

Figure 7-11 System Tree Window

The left most window pane shows the system tree. The system tree includes the connected SANbox 6142 routers and the following components for each router:

- FC Ports (see page 7-20)
- iSCSI Ports (see page 7-23)
- Discovered iSCSI Initiators (see page 7-31)
- FC Discovered Targets (see page 7-34)
- iSCSI Discovered Targets (see page 7-38)
- FCIP Routes (see page 7-39)

Select a component in the system tree to see component data in the tabbed pages to the right of the tree (see page 7-11).

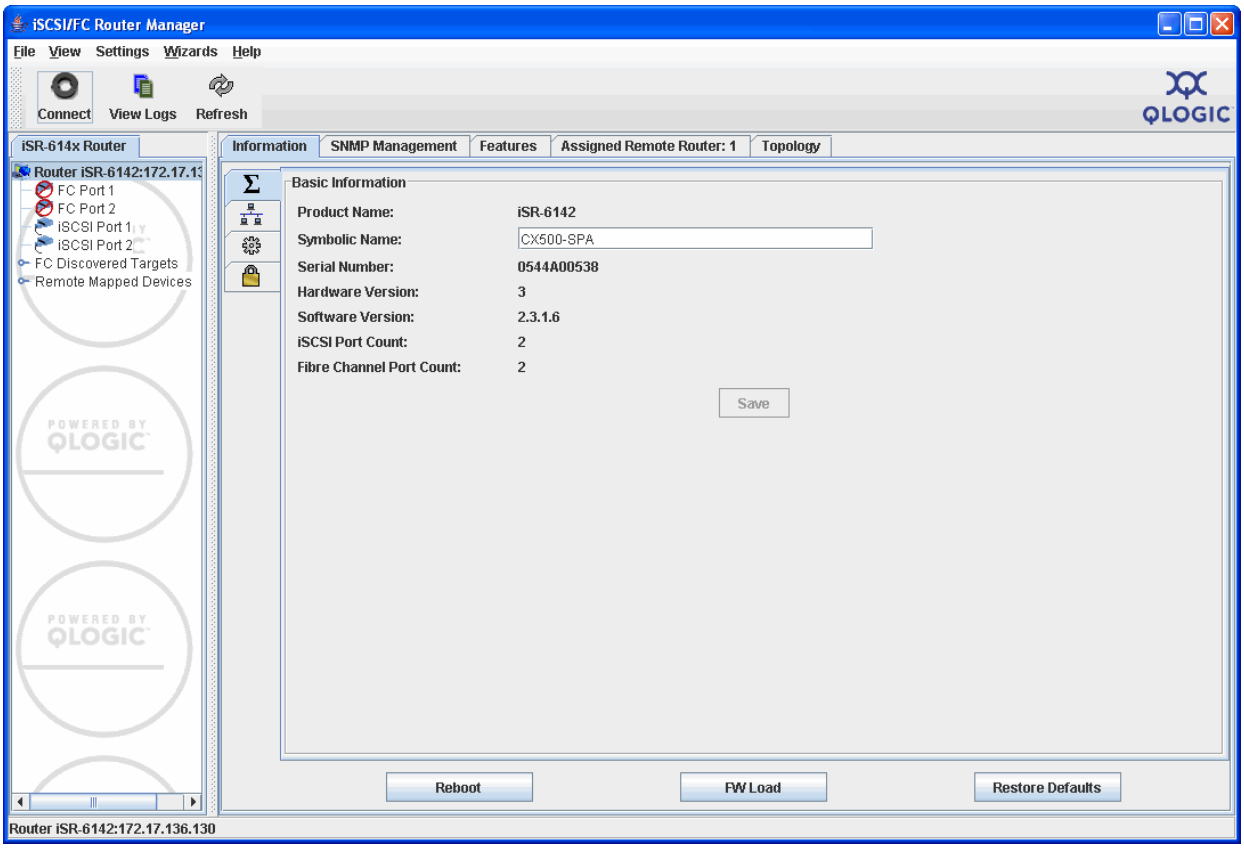


Figure 7-12 Component Information

Component information displayed for a selected router includes router information, configuration details, router status, and lists of connected or discovered devices.

SANbox 6142 Router

The top of the router tree displays the router system configuration and status. It contains the following tabs:

- Information Tab (see page 7-12)
- SNMP Management Tab (see page 7-17)
- Features Tab (see page 7-19)
- Assigned Remote Router Tab (see page 7-19)
- Topology Tab (see page 7-20)

NOTE:

If your router's configuration includes a remote router, the router configuration window includes a tab with the basic information for that router, as shown in the following example for **Assigned Remote Router:1**. You can define additional remote routers using the Add Remote Peer wizard.

Information Tab

The Information tab provides four vertical tabs with icons that identify its content: Basic Information, Management Information, and NTP Server Information, and Security. It also contains three buttons: **Reboot**, **FW Load**, and **Restore Defaults**.

Basic Information

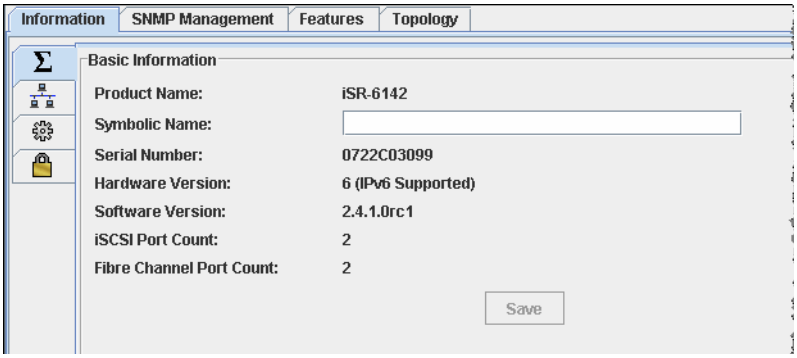


Figure 7-13 Basic Information Vertical Tab

The Basic Information tab provides the following parameters:

- **Product Name** – Identifies the router model.
- **Symbolic Name** – Lets you to assign a symbolic name to the router.
- **Serial Number** – Displays the router's serial number.

- **Hardware Version** – Identifies the router hardware version number.
- **Software Version** – Identifies the version of firmware loaded on the router.
- **iSCSI Port Count** – Identifies the number of iSCSI ports (2).
- **Fibre Channel Port Count** – Identifies the number of Fibre Channel ports (2).

Management Information

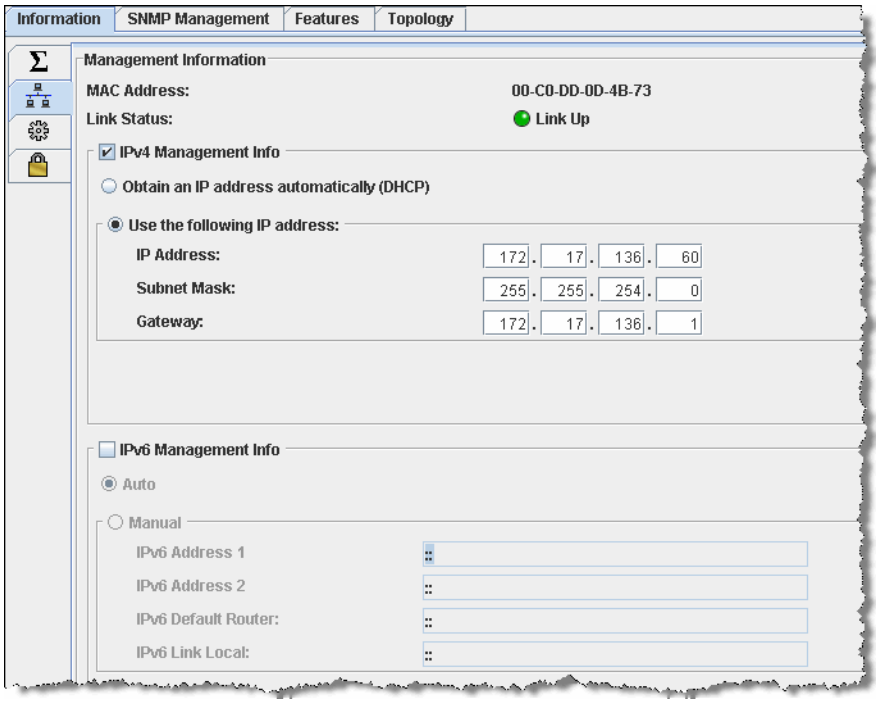


Figure 7-14 Management Information Vertical Tab

The Management Information tab provides the following parameters:

- **MAC Address** – Displays the management port's MAC address.
- **Link Status** – Displays the management port link status: **Link UP** or **Link Down**.

- **IPv4 Management Info** – Select this check box to use IPv4 (Internet Protocol version 4, 32-bit addressing), then use the radio buttons to identify whether to use either a dynamic or static IP address.
  - **IP Address** – Displays the management port's subnet mask.
    - If you selected the **Obtain an IP address automatically (DHCP)** radio button, the system obtains the IP address automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can configure the IP address.
  - **Subnet Mask** – Displays the management port's subnet mask.
    - If you select the **Obtain an IP address automatically (DHCP)**, the system obtains the subnet mask automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can configure the subnet mask.
  - **Gateway** – Displays the IP address of the server acting as a gateway to your Internet connection.
    - If you select the **Obtain an IP address automatically (DHCP)**, the system obtains the gateway address automatically through DHCP.
    - If you selected the **Use the following IP address** radio button, you can specify the gateway address.
- **IPv6 Management Info** – Select this check box to use IPv6 (Internet Protocol version 6, 128-bit addressing), then use the radio buttons to identify whether to use either a dynamic or static IP address.
  - **IPv6 Management Info –** Select this check box if you want to use IPv6, then use the radio buttons to identify whether to use a dynamic or static IP address.
  - **IPv6 Address1** – The first user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Address2** – The second user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.

- **IPv6 Default Router** – Use this address to set the default router for the IPv6. The system can also set the IPv6 default router dynamically depending on your network configuration.
- **IPv6 Local Link** – This field contains the IPv6 link local address of the port. It is not editable.

NOTE:

IPv6 support is available only with hardware version 6 and software version 2.4.0.0 and greater.

- **Set IP Address** – After making any IP address changes, click this button to save your changes.

NTP Server Information

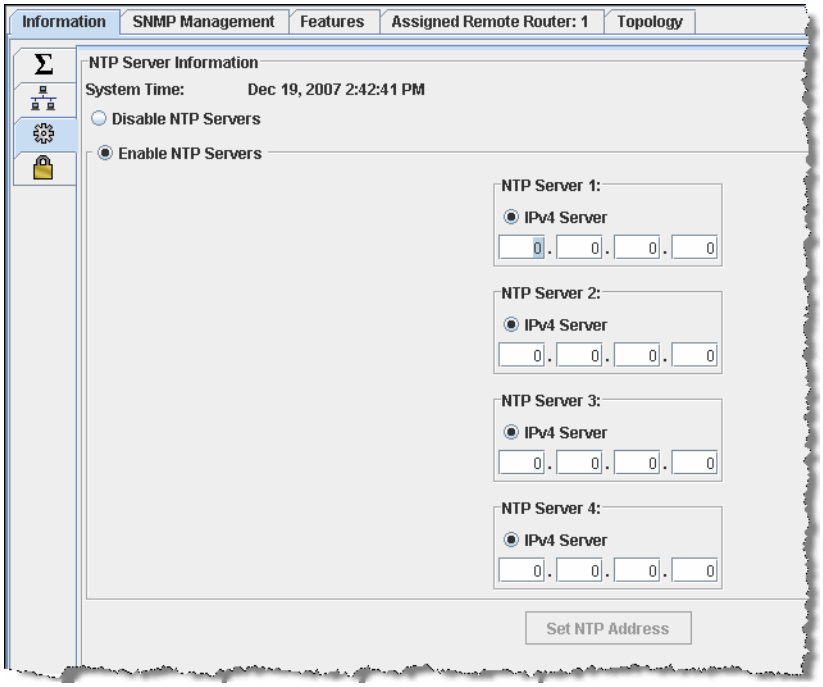


Figure 7-15 NTP Server Information Vertical Tab

The NTP Server Information tab provides the following parameters:

- **NTP Server Radio Buttons** – Use these buttons to disable or enable the use of NTP servers to set the router's date and time.
- **NTP Server 1** – Displays the IP address of the first NTP server to be queried by the router when setting its time and date.

- **NTP Server 2** – Displays the IP address of the second NTP server to be queried by the router when setting its time and date. This server is used only if the first NTP server did not respond.
- **NTP Server 3** – Displays the IP address of the third NTP server to be queried by the router when setting its time and date. This server is used only if the first and second NTP servers did not respond.
- **NTP Server 4** – Displays the IP address of the fourth NTP server to be queried by the router when setting its time and date. This server is used only if the first, second, and third NTP servers did not respond.
- **Set NTP Address** – After enabling NTP Servers and setting their IP addresses, click this button saves any changes made to the NTP server IP addresses.

Security

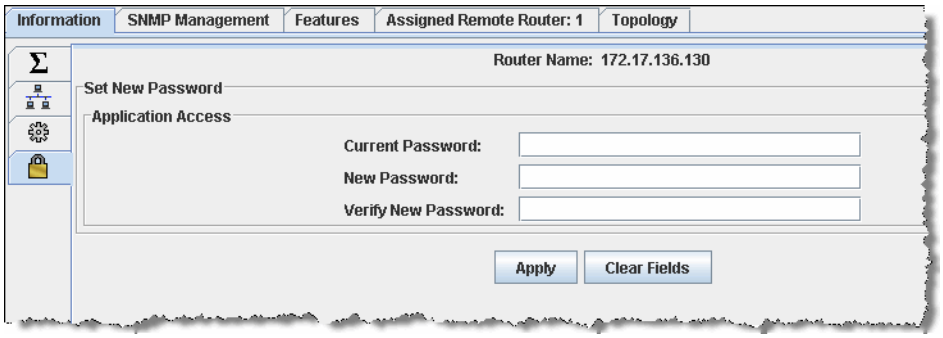


Figure 7-16 Security Vertical Tab

The Security tab enables you to set the router's password. The Security tab provides the following parameters:

- **Current Password** – You must enter the current password before changing it.
- **New Password** – Enter the new router password.
- **Verify New Password** – Verify the password entered in the New Password field.
- **Apply** – Click this button to save the password changes.
- **Clear Fields** – Click this button to clear the **Current Password**, **New Password**, and **Verify Password** fields.

SNMP Management Tab

The SNMP Management tabbed page consists of two sections: SNMP Configuration and SNMP Trap Receivers. The **Save** button saves any SNMP management changes. For more information, see Appendix D.

Figure 7-17 shows the SNMP Management tabbed page. The following paragraphs describe it.

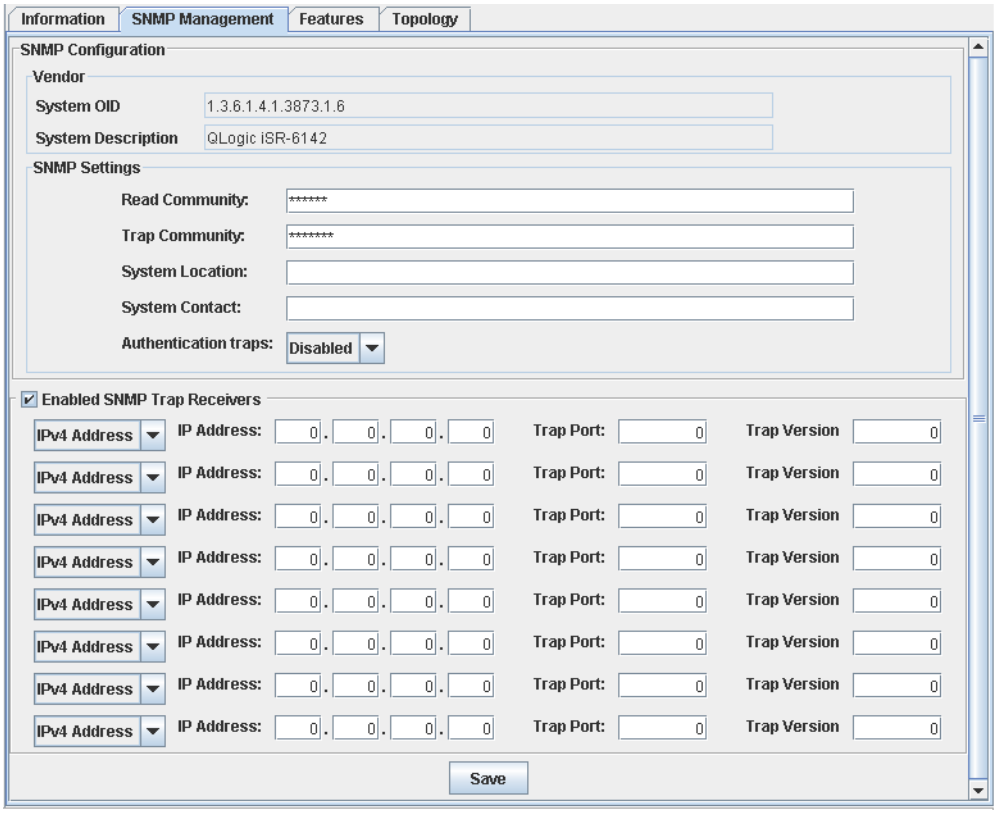


Figure 7-17 SNMP Management Tabbed Page

The SNMP Management tab provides two configuration sections:

- SNMP Configuration
- SNMP Trap Receivers

SNMP Configuration

The SNMP Configuration section provides the following vendor and SNMP setting fields:

- **System OID** – Displays the system object identifier.
- **System Description** – Displays a description of the router location.

- **Read Community** – Enter a password that authorizes an SNMP management server to read information from the router. This is a write-only field. The value on the router and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is public.
- **Trap Community** – Enter a password that authorizes an SNMP management server to receive traps. This is a write-only field. The value on the router and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding the number sign (#), semicolon (;), and comma (,). The default is public.
- **System Location** – Specifies the name of the router location. The name can be up to 64 characters excluding the number sign (#), semicolon (;), and comma (,).
- **System Contact** – Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding the number sign (#), semicolon (;), and comma (,).
- **Authentication Traps** – Enables or disables the generation of authentication traps in response to authentication failures.

SNMP Trap Receivers

- **Enabled** – Select this check box next to each trap receiver you want to configure, then use the following fields to specify its IP address, trap port, and trap version.
- **IP Protocol** – Select the IP protocol version from the drop-down menu: IPv6 Address or IPv4 Address. The IP address field changes to accept the appropriate format.
- **IP Address** – Specifies the IP address to which the SNMP traps are sent. A maximum of eight trap addresses are supported.
- **Trap Port** – Identifies the port number on which the trap is sent. The default is 162.
- **Trap Version** – Specifies the SNMP version (1 or 2) with which to format traps.

Features Tab

Figure 7-18 shows the Features tabbed page that displays the routers licensed features and lets you apply additional license features. The following paragraphs described the page.

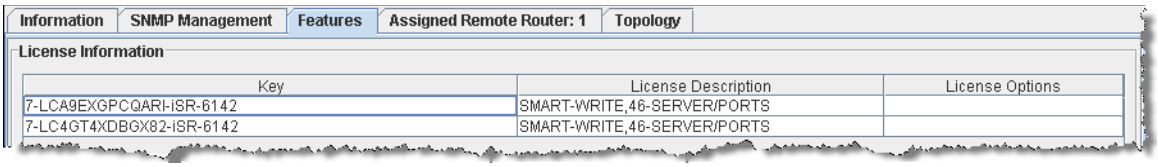


Figure 7-18 Features Tabbed Page

- **License Information** – Displays a list of the routers licensed features.
- **Add** – Initiates the Add Feature wizard.

Assigned Remote Router Tab

If your local router has any remote routers added as peers to its configuration, the SANbox 6142 router screen includes a tabbed page for each assigned remote router.

This screen provides the following information about the remote router:

- **Product Name** – Identifies the model of the remote router.
- **Symbolic Name** – Displays the symbolic name, if one is assigned to the remote router.
- **Serial Number** – Displays the remote router's serial number.
- **Hardware Version** – Identifies the remote router hardware version number. Starting with version 6, the hardware supports IPv6.
- **Software Version** – Identifies the version of firmware loaded on the remote router. IPv6 requires software version 2.4.0.0 or later.
- **iSCSI Port Count** – Identifies the number of iSCSI ports (2).
- **Management IP Address** – Displays the IP address of the remote router.

Topology Tab

Figure 7-19 shows the Topology tabbed page that displays the routers, as shown in the following example.

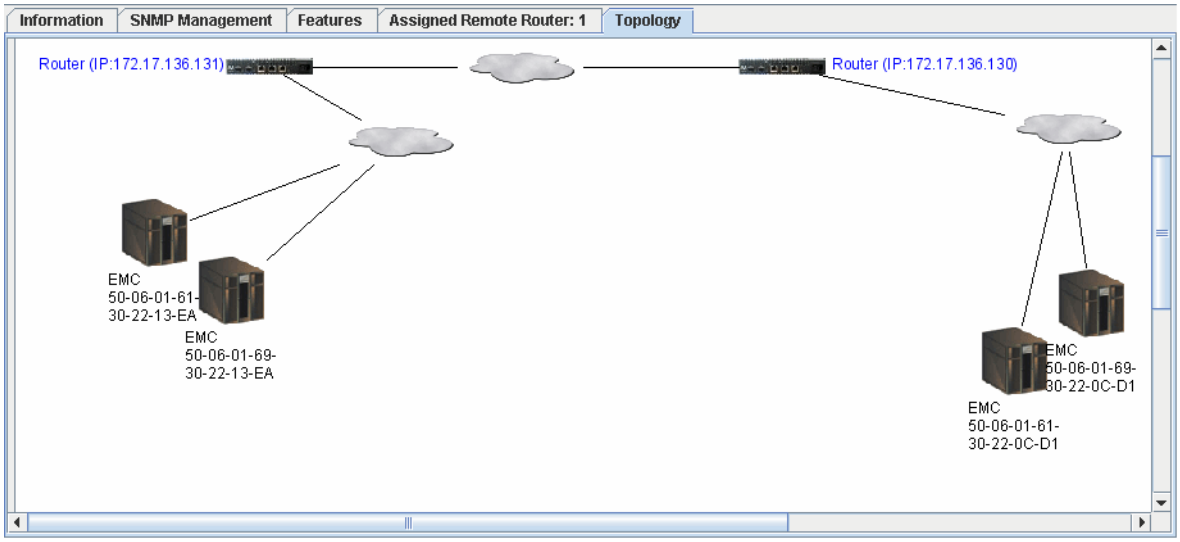


Figure 7-19 Topology Tabbed Page

FC Ports

When you select an FC port in the system tree, the system displays the FC Port Information tabbed page (see Figure 7-20).

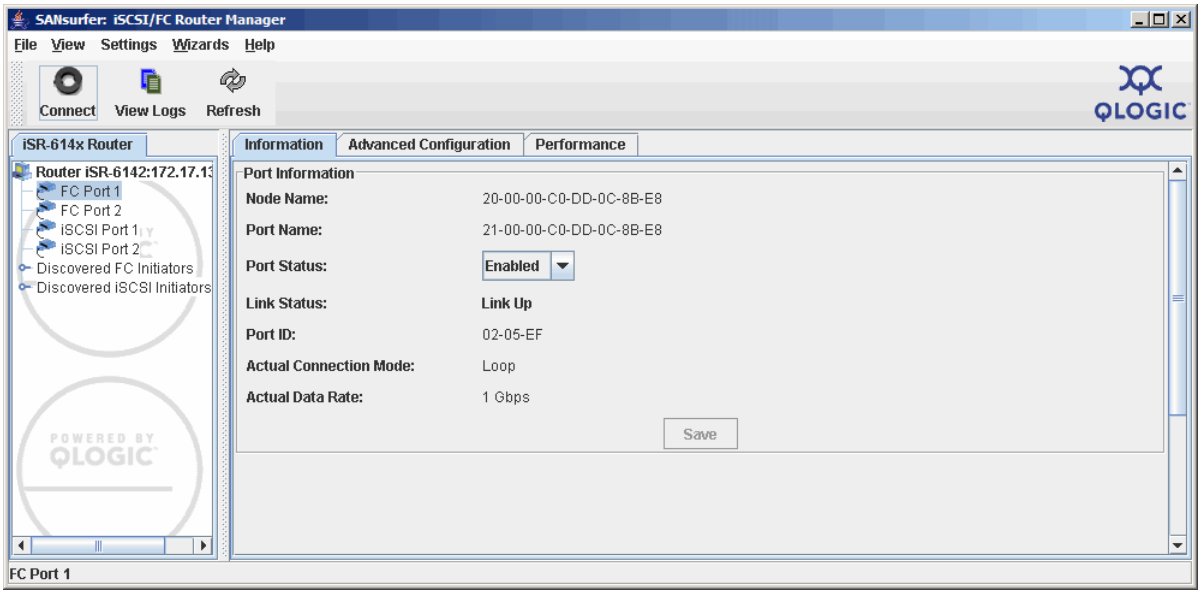


Figure 7-20 FC Port Information Tab

FC Port Information Tab

The FC Port Information tab provides the following parameters:

- **Node Name** – Displays the world-wide node name (WWNN) assigned to the FC port.
- **Port Name** – Displays the world-wide port name (WWPN) assigned to the FC port.
- **Port Status** – Lets you change the port status: **Enabled** (online) or **Disabled** (offline). After changing the status, click **Save**. If you choose to disable the port, a warning message appears, letting you know it will disconnect one or more ports. Click **Yes** to disconnect the port, or **No** to cancel the changes.
- **Link Status** – Displays the link status, either `Link Up` or `Link Down`.
- **Port ID** – Displays the ID assigned by the FC fabric or AL_PA if the FC port is connected to a private loop.
- **Actual Connection Mode** – Displays the port's connection mode, either point-to-point or loop.
- **Actual Data Rate** – Displays the port's operating data rate when online, either one gigabit per second (1 Gbps) or two gigabits per second (2 Gbps).

FC Port Advanced Configuration Tab

When you select the **Advanced Configuration** tab for the selected FC port, the system displays the Advanced Configuration tabbed page (see Figure 7-21).

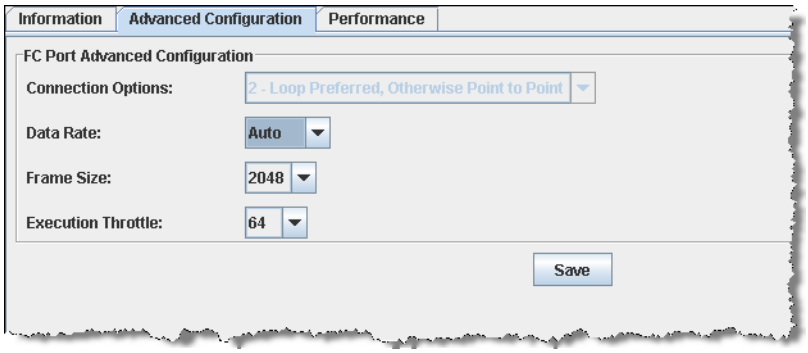


Figure 7-21 FC Port Advanced Configuration Tab

The FC port Advanced Configuration tab provides the following parameters:

- **Connection Options** – Displays the connections. When an FC port is not part of an FCIP route, it only operates in FC loop mode.
- **Data Rate** – Displays a drop-down list that lets you set the data rate: **Auto**, **1 Gbps**, or **2 Gbps**. The default is auto. If you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

- **Frame Size** – Displays a drop-down list that lets you set the frame size: **2048**, **1024**, or **512** bytes. The default is **2048**. If you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Execution Throttle** – Displays a drop-down list that lets you set the execution throttle: **16**, **32**, **64**, **128**, or **256**. The default is **64**. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

FC Port Performance Tab

When you select the **Performance** tab for the selected FC port, the system displays the Performance tabbed page (see Figure 7-22).

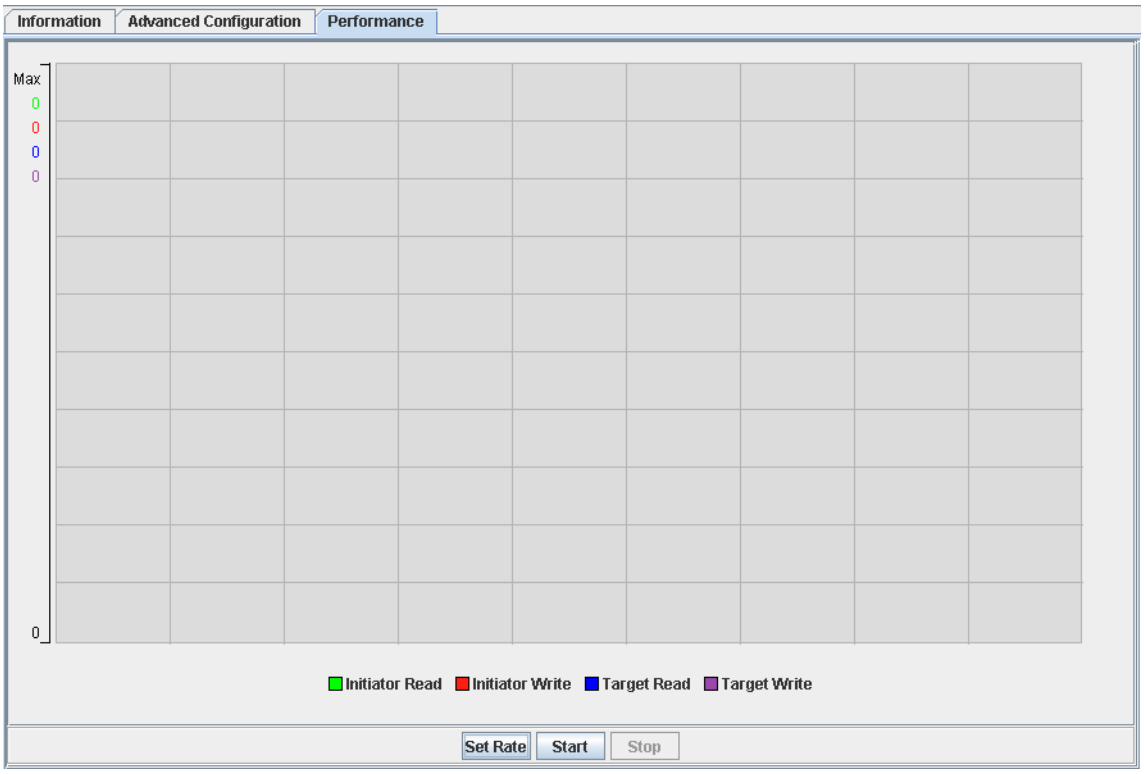


Figure 7-22 FC Port Performance Tab

The FC Port Performance tab displays the following information:

- **Initiator Read** – Shows the initiator's read performance through the selected FC port.
- **Initiator Write** – Shows the initiator's write performance through the selected FC port.
- **Target Read** – Shows the target's read performance through the selected FC port.

- **Target Write** – Shows the target's write performance through the selected FC port.

iSCSI Ports

When you select an iSCSI port in the system tree, the window displays the Information, Advanced Configuration, and Statistics tabbed pages to the right of the tree (see Figure 7-23). These following sections describe these pages.

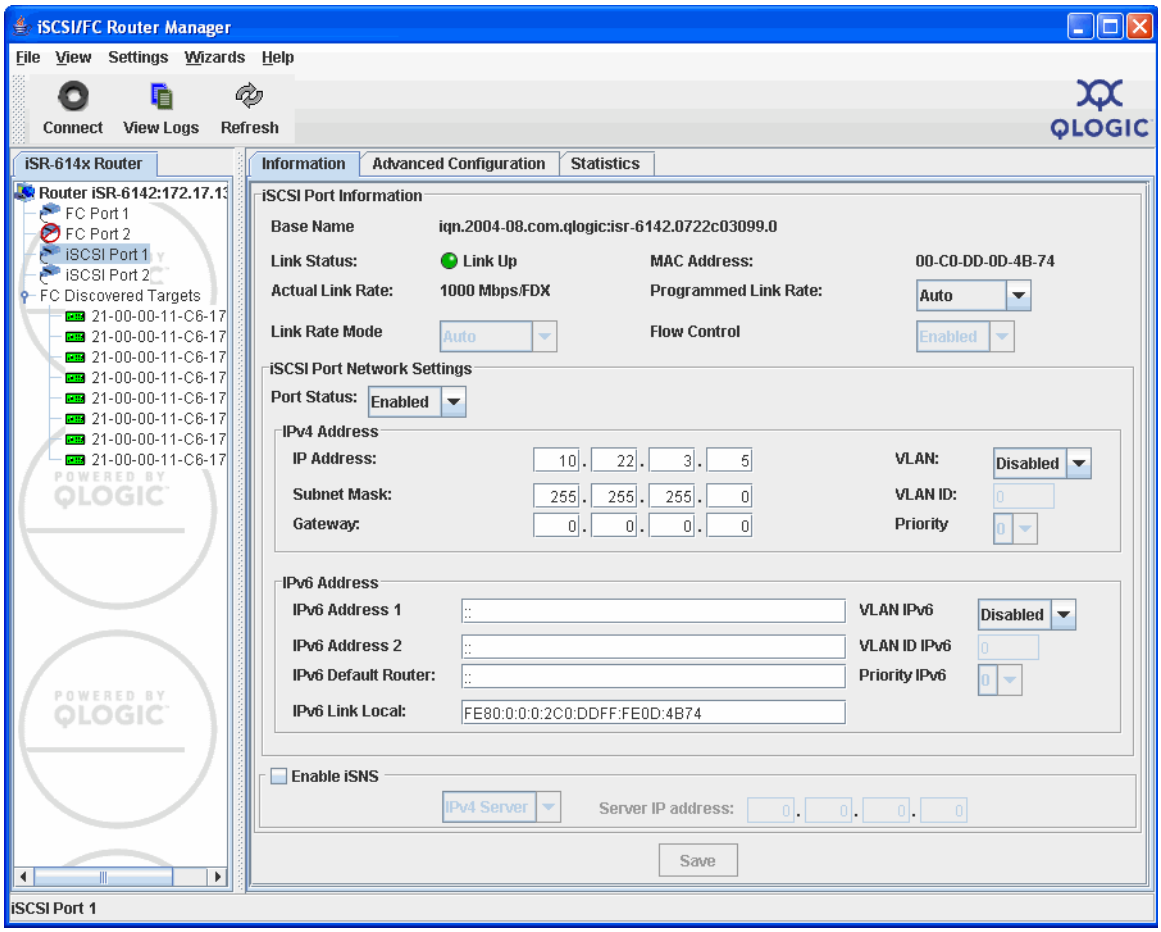


Figure 7-23 iSCSI Port Tabbed Pages

Information Tab

The Information tabbed page consists of three areas: Port Information, iSCSI Port Network Settings, and iSNS. The following paragraphs describe the information displayed in these sections.

iSCSI Port Information

The iSCSI Port Information area provides the following parameters:

- **Base Name** – Displays the full name assigned to the selected iSCSI port.
- **Link Status** – Identifies the port connection status: `Link Up` or `Link Down`.
- **MAC Address** – Displays the MAC address assigned to the port. The MAC address is not changeable.
- **Actual Link Rate** – Displays the actual link rate, which can be `Unknown`, `1000 Mbps`, `100 Mbps`, or `10 Mbps`. If the port's configuration or connection has changed, the status may not be current. Click the **Refresh** icon to display the current status.
- **Programmed Link Rate** – The configured data rate for the port. To configure the data rate, open the drop-down menu and select one of the following data rates:
  - **Auto** - Data rate determined by network attachment
  - **10 Mbps** - 10 megabits per second
  - **100 Mbps** - 100 megabits per second
  - **1000 Mbps** - 1000 megabits per second (1 gigabit per second)

  When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Link Rate Mode** – If you selected a specific **Programmed Link Rate** (not **Auto**), you can specify one of these modes:
  - **Auto**
  - **Half Duplex**
  - **Full Duplex**
- **Flow Control** – If you selected a specific **Programmed Link Rate** (not **Auto**), you can enable or disable flow control.

iSCSI Port Network Settings

- **Port Status** – When the port link is up, you can enable or disable the port using this drop-down list.
- **IPv4 Address** – When using an IPv4 address scheme, define the following fields:
  - **IP Address** – The IP address to which the port responds. An un-initialized port has an IP address of all zeros. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **Subnet Mask** – The subnet mask used by the port. Although you may modify the subnet mask in this window, you will typically set it using the Configuration Wizard.
  - **Gateway** – The gateway for the selected port.
  - **VLAN** – The VLAN configuration: **Disabled** or **Enabled**. You can configure VLAN from this window.
  - **VLAN ID** – When VLAN is enabled the VLAN ID contains an identification value in the range 0 to 4094. You can configure VLAN from this window.
  - **Priority** – When VLAN is enabled, this field defines the priority assigned to this VLAN. To set the priority, open the drop-down menu and select the desired value (between 0 to 7).
- **IPv6 Address** – When using an IPv6 address scheme, define the following fields:
  - **IPv6 Address1** – The first user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Address2** – The second user-assigned IPv6 address to which the port responds. A value of :: indicates that an IPv6 address has not been assigned. Although you may modify the IP address in this window, you will typically set it using the Configuration Wizard.
  - **IPv6 Default Router** – Use this address to set the default router for the IPv6. The system can also set the IPv6 default router dynamically depending on your network configuration.
  - **IPv6 Local Link** – This field contains the IPv6 link local address of the port. It is not editable.
  - **VLAN IPv6** – The VLAN IPv6 configuration: **Disabled** or **Enabled**. You can configure VLAN from this window.

- **VLAN ID IPv6** – When VLAN IPv6 is enabled the VLAN ID IPv6 contains an identification value in the range 0 to 4094. You can configure VLAN from this window.
- **Priority IPv6** – When VLAN IPv6 is enabled, this field defines the priority assigned to this VLAN IPv6. To set the priority, open the drop-down menu and select the desired value (between 0 to 7).

NOTE:

IPv6 support is available only with hardware version 6 and greater and software version 2.4.0.0 and greater.

- **Enable iSNS** – This check box enables or disables iSNS support. Select the check box to enable this option; clear the check box to disable it.
  - **IP Server –** This drop-down box lets you choose the IP address version assigned to the IP server. The following examples show the IP address fields that open when you choose one of these options.
  - **Server IP Address** – The IP address assigned to the iSNS server to which this port will communicate. You can configure this IP address when iSNS is enabled. Note the different formats provided for the two different IP address version.

Advanced Configuration Tab

The Advanced Configuration tabbed page allows you to configure the router's port parameters, security settings, and CHAP settings. The information displayed in these sections is illustrated in Figure 7-24 and described in the following paragraphs.

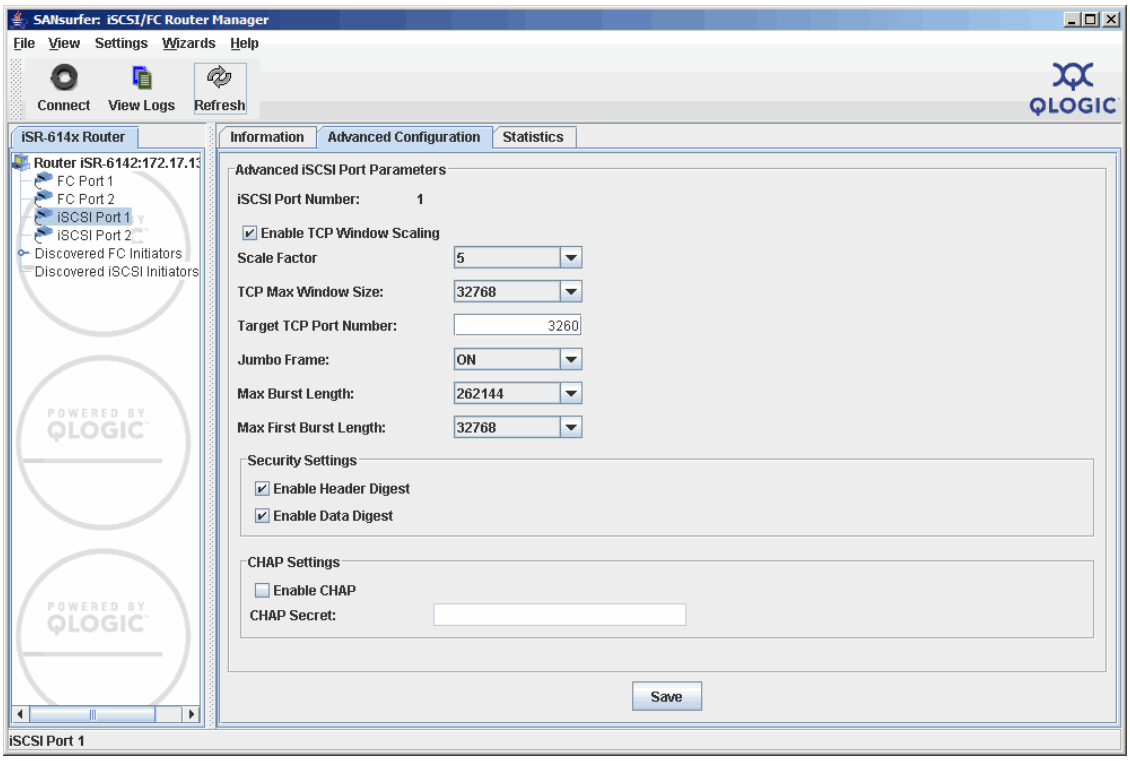


Figure 7-24 Advanced Configuration Tabbed Page

The iSCSI Port Advanced Configuration tab provides the following parameters:

- **iSCSI Port Number** – Identifies the iSCSI port number (1 or 2).
- **Enable TCP Window Scaling** – When you change this setting, you must enter the **Scale Factor** (valid values are `0`–`5`), then click **Save** (at the bottom of the page) for the change to take effect.
- **TCP Max Window Size** – Enables you to set the TCP maximum window size. To change the setting, open the drop-down menu and select one of the options: `8192`, `16384`, or `32768`.

- **Target TCP Port Number** – Identifies the TCP port number the router uses to receive iSCSI target commands. The iSCSI community uses TCP port number `3260` by default any change to this TCP port number requires a corresponding change in all iSCSI initiators connecting to this iSCSI target port. When you change the target TCP port number, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Jumbo Frame** – Enables or disables router jumbo frame size as the maximum transfer unit (MTU). Disabling this option sets the port to support `1500` byte MTU. Enabling this option sets the port to support `9000` bytes MTU. To change this setting, select **Enabled** or **Disabled** from the drop-down menu. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
- **Max Burst Length** – Enables you to set the iSCSI maximum burst length. To change this setting, select the desired value (ranging from `512` to `262144` bytes) from the drop-down menu.
- **Max First Burst Length** – Enables you to set the iSCSI maximum first burst length. To change this setting, select the desired value (ranging from `512` to `262144` bytes) from the drop-down menu.
- **Security Settings**
  - **Enable Header Digest** – Enables or disables support for iSCSI header digest. Header digest is an ISCSI feature that adds a validity check field to iSCSI PDU headers to verify that no corruption has occurred during the transmission of the PDU header. The SANbox 6142 router supports digest in its hardware to maximize performance. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
  - **Enable Data Digest** – Enables or disables support for iSCSI data digest. Data digest is an ISCSI feature that adds a validity check to iSCSI data to verify that no corruption has occurred during the transmission of the data. The SANbox 6142 router supports data digest in its hardware to maximize performance. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.

- **CHAP Settings**
  - **Enable CHAP** – Enables or disables CHAP (Challenge Handshake Authentication Protocol) support. Select the check box to enable this option; clear the check box to disable it. When you change this setting, you must click **Save** (at the bottom of the page) for the change to take effect.
  - **CHAP Secret** – Lets you define the CHAP secret used for authenticating an iSCSI client. The field is available only when the Enable CHAP check box is checked. When you change the **CHAP Secret** setting, you must click **Save** (at the bottom of the page) for the change to take effect.

Statistics Tab

The Statistics tabbed page consists of a scrollable table of parameters and values. The table is divided into two sections: the first section contains statistics that are port specific, and the second section contains shared statistics (common to both iSCSI ports).

You can refresh the statistics are by clicking **Refresh** at the top of the scrollable window. You can clear the statistics (set all values to zero) by clicking **Clear**.

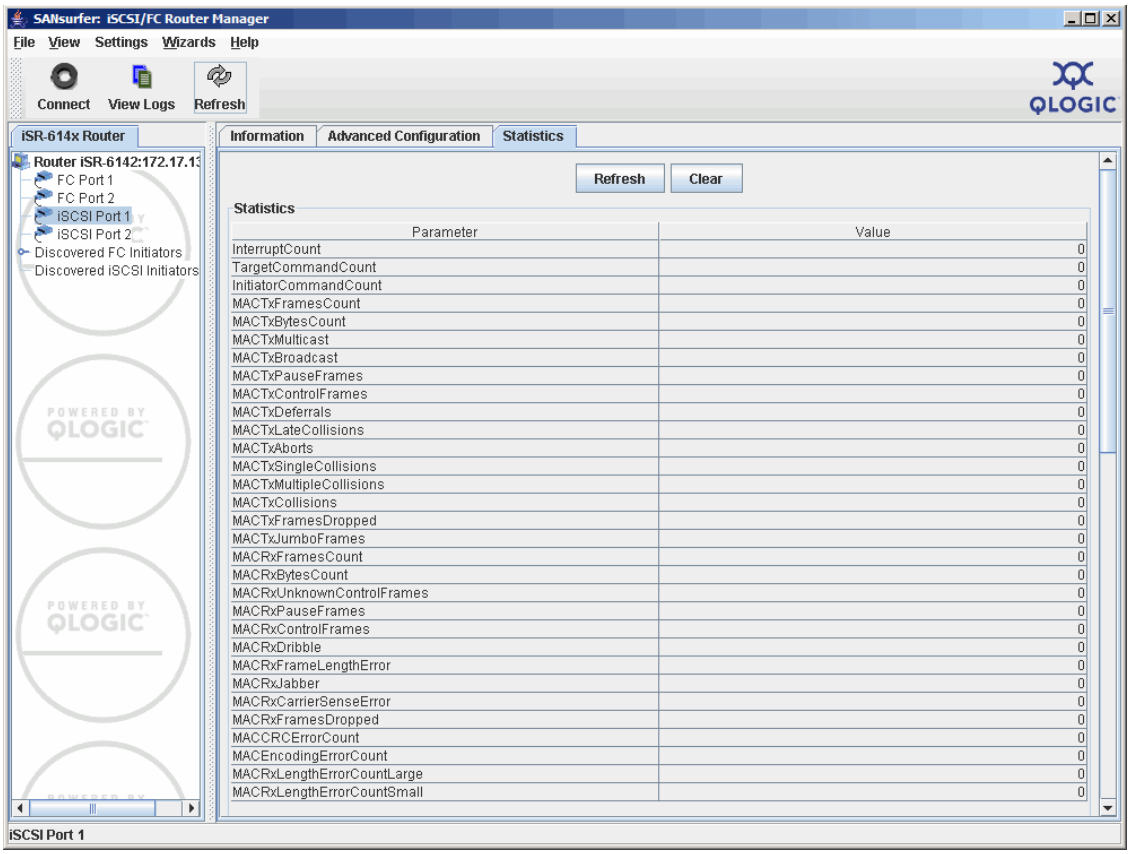


Figure 7-25 iSCSI Statistics Tabbed Page

Discovered iSCSI Initiators

Selecting the Discovered iSCSI Initiators branch on the system tree does not provide any information in the right window. Select a discovered iSCSI initiator in the system tree to display the Information and LUN List tabbed pages to the right of the system tree, which are shown in Figure 7-26 and described in the following sections.

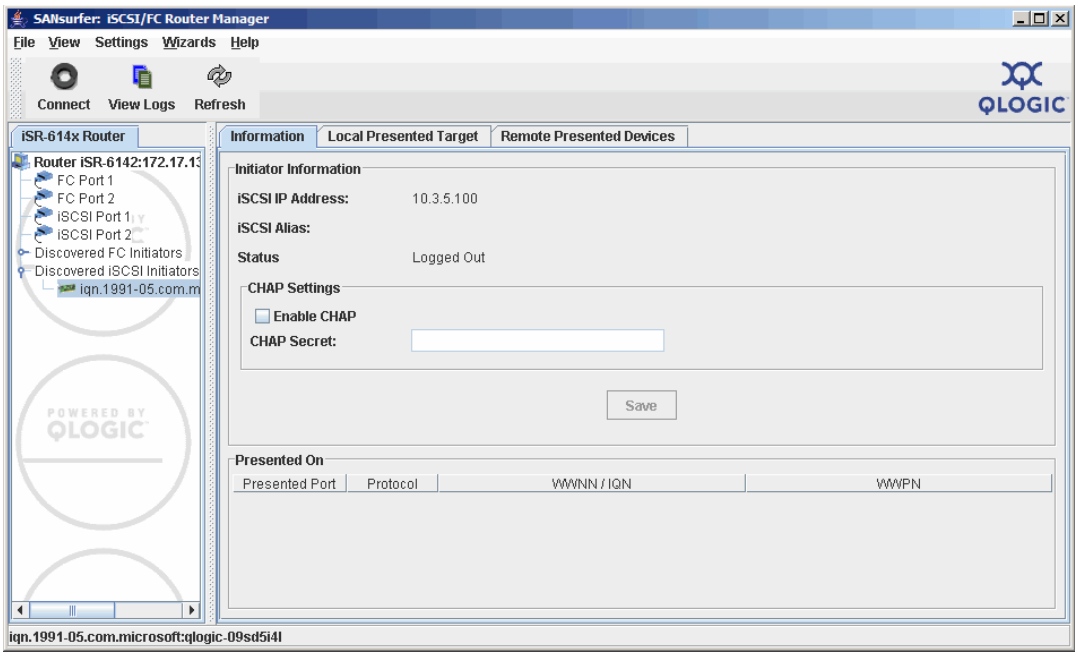


Figure 7-26 Discovered iSCSI Initiator Tabbed Pages

Information Tab

The Information tabbed page consists of two sections: Initiator Information and CHAP Settings. The following paragraphs describe the information displayed in these sections.

The **Initiator Information** section provides the following parameters:

- **iSCSI IP Address** – Displays the IP address of the discovered iSCSI initiator.
- **iSCSI Alias** – Displays the iSCSI initiators alias, which the initiator provides when it logs into the iSR-6142 router.
- **Status** – Displays the activity status for the selected initiator.

The CHAP Settings section provides the following parameters:

- **Enable CHAP** – Enables or disables CHAP (Challenge Handshake Authentication Protocol) support. Select the check box to enable this option; clear the check box to disable it.
- **CHAP Secret** – Lets you define the CHAP secret used for authenticating an iSCSI client. The field is available only when the CHAP check box is checked.

NOTE:

To apply any changes, click the **Save** button, located at the bottom of window.

Local Presented Target Tab

The Local Presented Target tabbed page consists of a scrollable list of logical unit numbers (LUNs) mapped to the iSCSI initiator, as shown in Figure 7-27 and described in the following paragraphs.

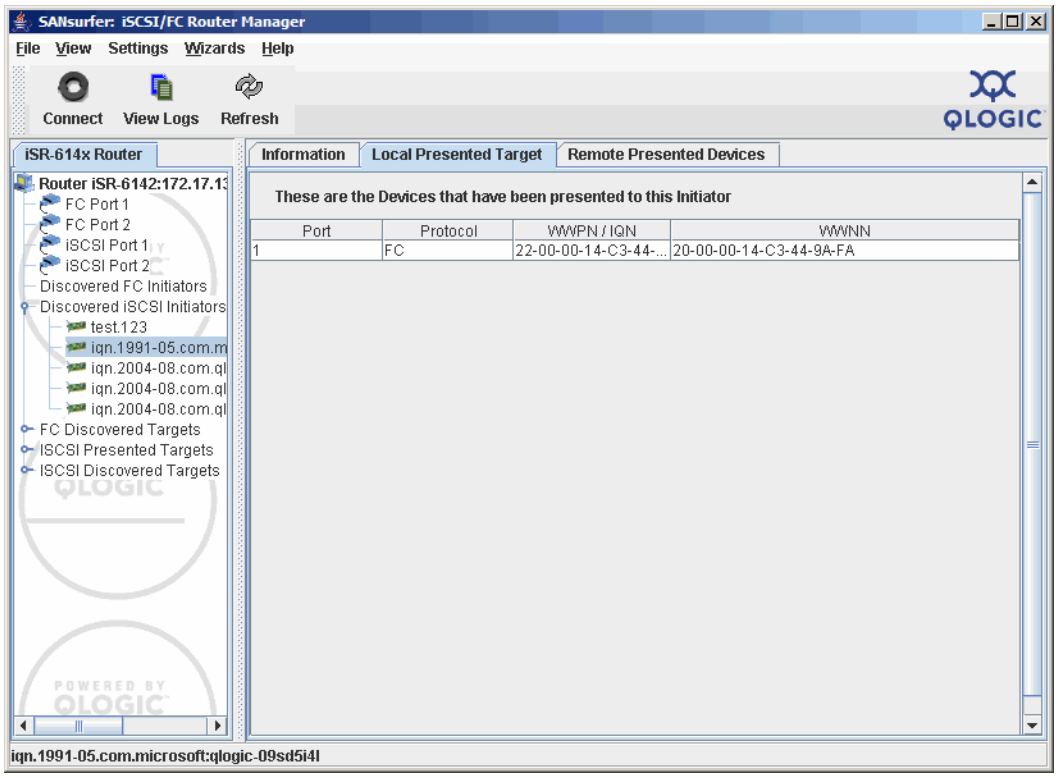


Figure 7-27 Local Presented Target Tabbed Page

- **Port** – Displays information provided by the target LUN as a result of issuing a SCSI Inquiry command.
- **Protocol** – Identifies the target name. For FC targets, the name is the WWPN.
- **WWPN/IQN** – Specifies the world wide unique LUN name (WWULN), also provided on page 83 of a SCSI Inquiry command.
- **WWNN** – Shows the logical unit number.

Remote Presented Target Tab

The Remote Presented Target tabbed page consists of a scrollable list of LUNs mapped to the iSCSI initiator, as shown in Figure 7-28 and described in the following paragraphs.

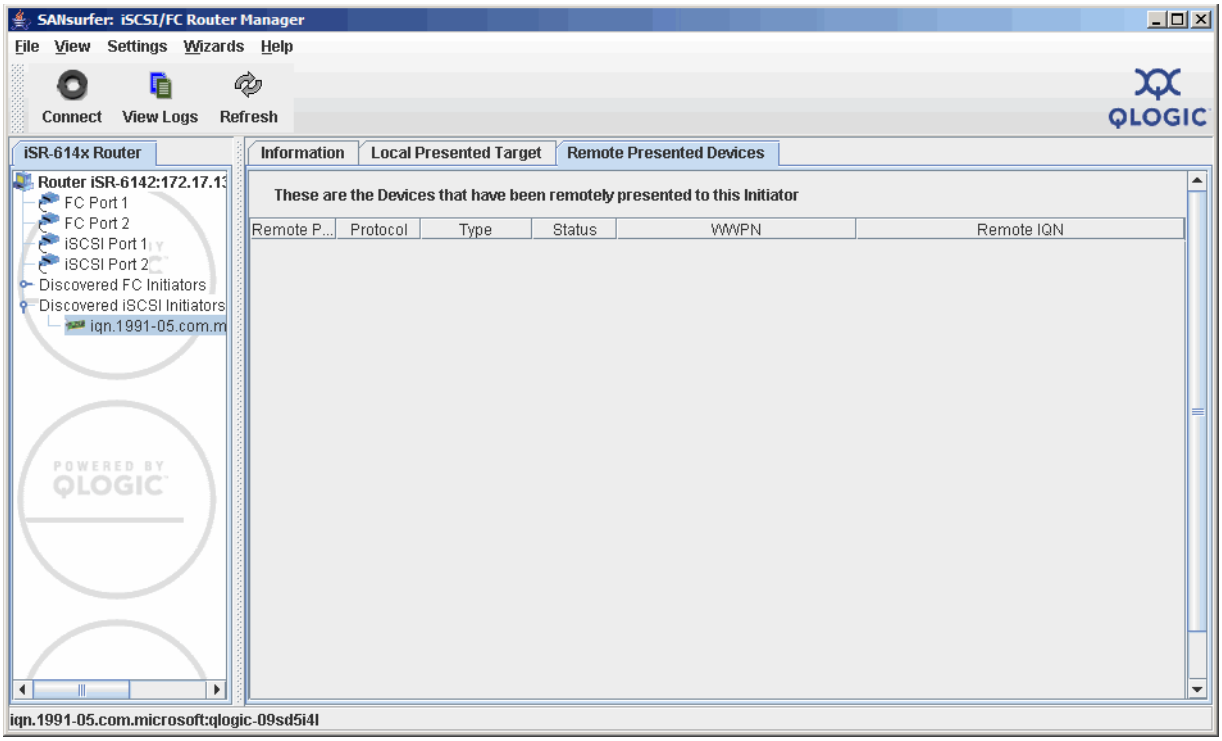


Figure 7-28 Remote Presented Target Tabbed Page

- **Remote Port** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Protocol** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Type** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.

- **Status** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **WWPN** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.
- **Remote IQN** – Displays information provided by the target LUN in response to the router issuing a SCSI Inquiry command.

FC Discovered Targets

Selecting an FC discovered target in the system tree does not provide any information in the right window. Select a discovered FC target to display the Information and Remote Presented Devices tabbed pages to the right of the system tree (see Figure 7-29).

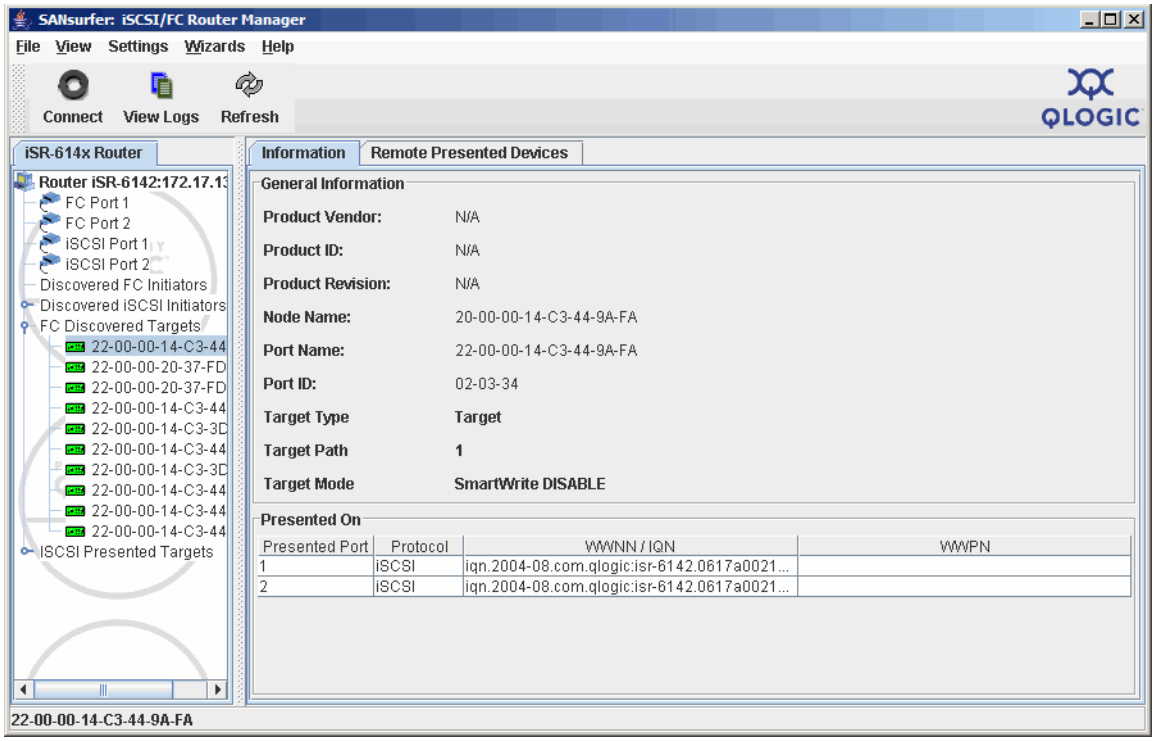


Figure 7-29 FC Discovered Targets Tabbed Pages

Information Tab

The Information tabbed page provides the following information about the selected FC target:

- **Product Vendor** – Displays the product vendor as reported by the SCSI Inquiry command.
- **Product ID** – Displays the product ID as reported by the SCSI Inquiry command.
- **Product Revision** – Displays the product revision as reported by the SCSI Inquiry command.
- **Node Name** – Displays the world-wide node name of the target device.
- **Port Name** – Displays the world-wide port name of the target device.
- **Port ID** – Displays the target device's port ID.

Remote Presented Devices Tab

The Remote Presented Devices tabbed page provides detailed target information and a scrollable list of LUNs, as shown in Figure 7-30 and described in the following paragraphs.

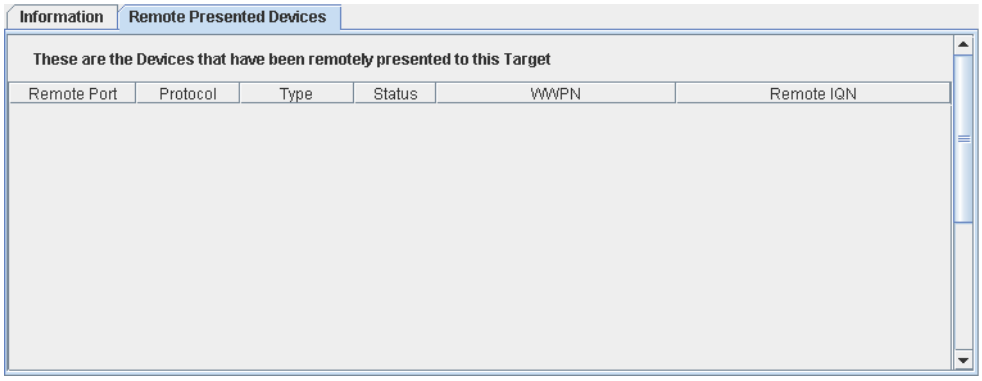


Figure 7-30 Remote Presented Devices Tab

- **General Information**
  - **Product Vendor** – Displays the vendor name of the target device as reported by the SCSI Inquiry command.
  - **Product ID** – Displays the product ID of the target device as reported by the SCSI Inquiry command.
  - **Product Revision** – Displays the product revision of the target device as reported by the SCSI Inquiry command.
  - **Node Name** – Displays the world-wide node name of the target device.

- **Port Name** – Displays the world-wide port name of the target device.
- **Port ID** – Displays the target device's port ID.
- **Target Type** – Displays the FC port where the target device was discovered.
- **Target Path** – Displays the logical unit number.
- **Target Mode** – Displays the vendor name of the LUN as reported by the SCSI Inquiry command.

- **Presented On** – Displays the product ID of the LUN as reported by the SCSI Inquiry command.
  - **Presented Port** – Displays the product revision of the LUN as reported by the SCSI Inquiry command.
  - **Protocol** – Displays the protocol in use, either iSCSI or FC.
  - **WWNN/IQN** – Displays the WWULN of the LUN as reported on page 83 of the SCSI Inquiry command.
  - **WWPN** – Displays the capacity (in megabytes) of the LUN as reported by the SCSI Capacity command.

iSCSI Presented Target List Tabbed Page

The **iSCSI Presented Target List** tabbed page provides detailed FC target information and a scrollable list of the iSCSI presentations of the target, as shown in Figure 7-31 and described in the following paragraphs.

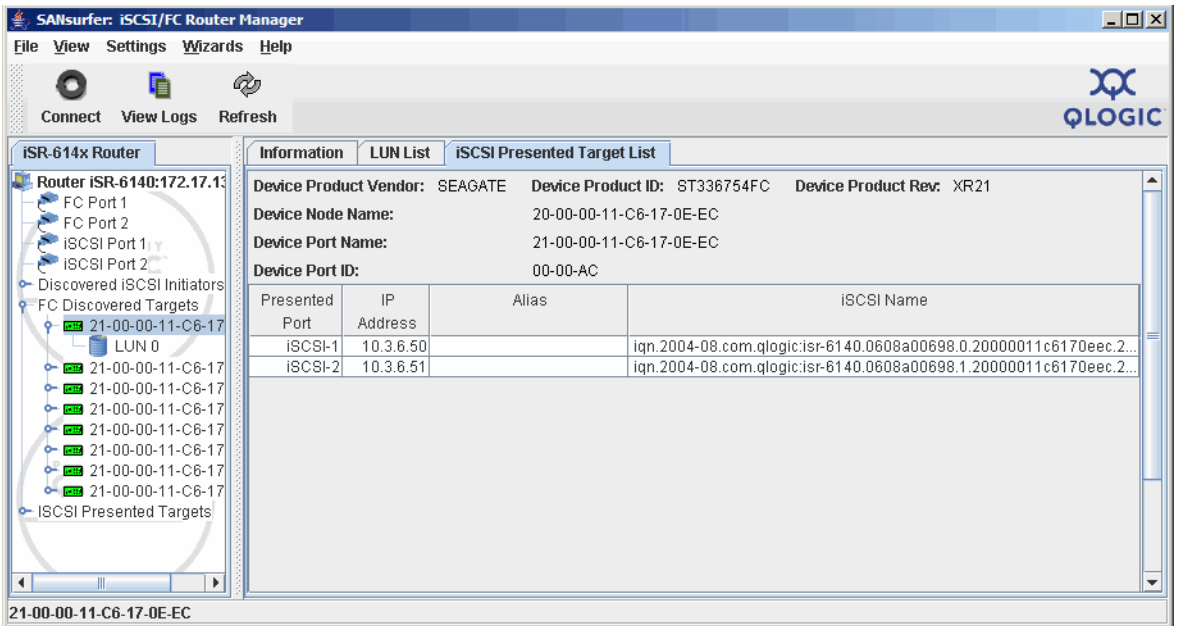


Figure 7-31 iSCSI Presented Target List Tabbed Page

- **Device Product Vendor** – Displays the vendor name of the target device as reported by the SCSI Inquiry command.
- **Device Product ID** – Displays the product ID name of the target device as reported by the SCSI Inquiry command.
- **Device Product Rev** – Displays the product revision of the target device as reported by the SCSI Inquiry command.
- **Device Node Name** – Displays the world-wide node name of the target device.
- **Device Port Name** – Displays the world-wide port name of the target device.
- **Device Port ID** – Displays the target device's port ID.
- **Presented Port** – Displays the iSCSI port number where the target is presented (1 or 2).
- **IP Address** – Displays the IP address on which the target is presented.
- **Alias** – Displays the iSCSI alias of the presented target.
- **iSCSI Name** – Displays the presented target's iSCSI name.
- **Size** – Displays the capacity (in megabytes) of the LUN as reported by the SCSI Capacity.

iSCSI Discovered Targets

The iSCSI Discovered Targets branch on the system tree does not provide any information in the right window. Select a discovered target to display the **Information** tabbed page to the right of the system tree (see Figure 7-32).

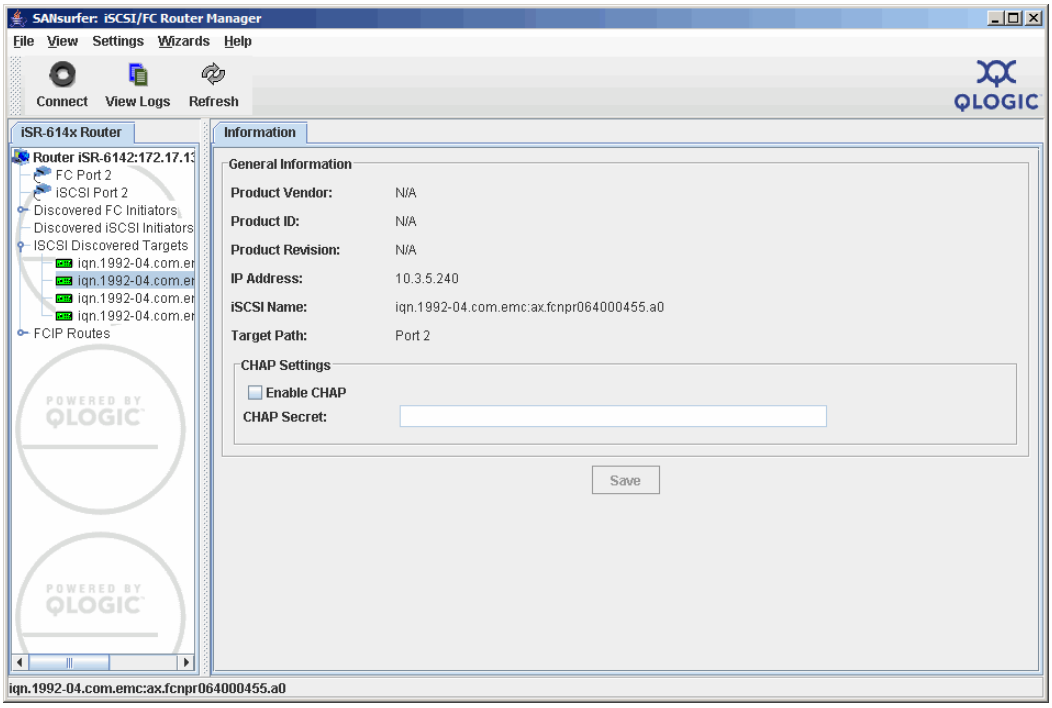


Figure 7-32 iSCSI Discovered Targets Tabbed Pages

Information Tabbed Page

The **Information** tabbed page consists of two sections: General Information and CHAP Settings, which are described in the following paragraphs.

- **General Information**
  - **Product Vendor** – Displays the product vendor as reported by the SCSI Inquiry command.
  - **Product ID** – Displays the product ID as reported by the SCSI Inquiry command.
  - **Product Revision** – Displays the product revision as reported by the SCSI Inquiry command.
  - **IP Address** – Displays the IP address of the presented iSCSI target.
  - **iSCSI Name** – Displays the presented iSCSI target's name.

- **Target Path** – Displays the router's iSCSI port where the target was discovered.

- **CHAP Settings** – Provides an option you can use to set the challenge handshake authentication protocol (CHAP) option as follows:
  - **Enable CHAP** – Select this check box to enable CHAP when connecting to this target.
  - **CHAP Secret –** When the **Enable CHAP** option is enabled, you can enter the string used for the CHAP secret when connecting to this target.

NOTE:

If you change the **CHAP Settings**, you must click **Save** for the change to take effect.

FCIP Routes

Selecting the FCIP Routes branch on the system tree does not provide any information in the right window. Select an **FCIP Route Info #** in the system tree to display the branch to display the **FCIP Route Information** and **Statistics** tabbed pages to the right of the system tree.

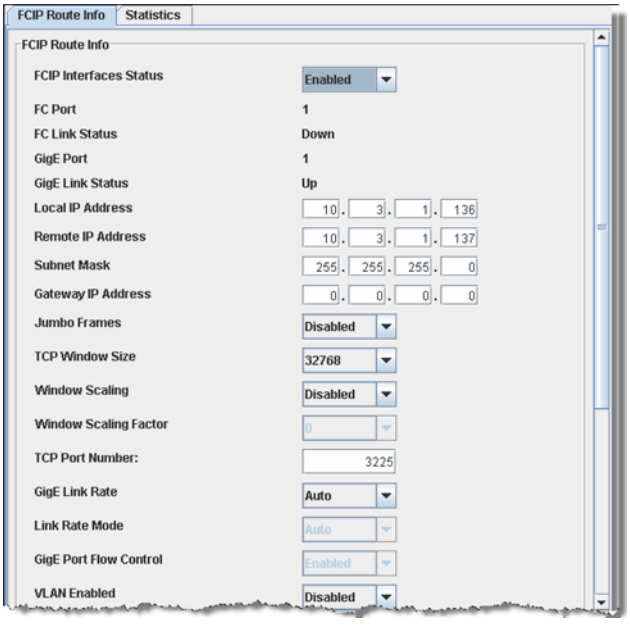


Figure 7-33 FCIP Route Tabbed Pages

FCIP Route Information Tabbed Page

The FCIP Route Information tabbed page contains the information that defines the selected FCIP route, as described in the following paragraphs.

- **FCIP Interface Status** – Provides a drop-down box you can use to enable or disable the FCIP route. Disabling the route places the FC and GE ports in a down state, but still retains all route configuration parameters.
- **FC Port** – Identifies the FC port assigned to the FCIP route when it was created.
- **FC Link Status** – Shows the state of the FC port used in this FCIP route.
- **GigE Port** – Identifies the gigabit Ethernet (GigE) port assigned to the FCIP route when it was created.
- **GigE Link Status** – Shows the state of the GigE port used in this FCIP route.
- **Local IP Address** – Fields you can use to define the IP address to be used by the GigE port. An uninitialized port has an IP address of all zeros.
- **Remote IP Address** – Fields you can use to define the IP address of the GigE port on the remote router.
- **Subnet Mask** – Fields you can use to define the subnet mask used by the GigE port.
- **Gateway IP Address** – Fields you can use to define the gateway IP address used by the GigE port.
- **Jumbo Frames** – Provides a drop-down box you can use to enable or disable Jumbo IP frames. When disabled, the MTU is 1500 bytes; when enabled, the maximum MTU is 9000 bytes.
- **TCP Window Size** – Provides a drop-down box you can use to choose one of three options for TCP window size: 8192, 16384, or 32768 bytes. The default is 32768.
- **Window Scaling** – Provides a drop-down box you can use to enable or disable TCP window scaling. The default is disabled.
- **Window Scaling Factor** – When **Window Scaling** is enabled, use this drop-down box to choose one of six options for TCP window scaling: 0–5.
- **TCP Port Number** – Field you can use to define the TCP port number.
- **GigE Link Rate** – Provides a drop-down box from which you can choose the link rate of the GigE port from one of four options: Auto, 10 Mbps, 100 Mbps, or 1000 Mbps.
- **Link Rate Mode** – When the GigE Link Rate is set to something other than auto, use this drop-down box to choose one of three options for the link rate mode: auto, half duplex, or full duplex.

- **GigE Port Flow Control** – When the GigE Link Rate is set to something other than auto, use this drop-down box to enable or disable GigE port flow control. The default is enabled.
- **VLAN Enabled** – Provides a drop-down box you can use to enable or disable VLAN support. The default is disabled.
- **VLAN ID** – When VLAN is enabled, use this field to define the VLAN ID. The VLAN ID must be the same on both routers participating in the FCIP route (local and remote routers must be using same VLAN ID) and the Ethernet switches.
- **VLAN Priority** – When VLAN is enabled, use this drop-down box to set the VLAN priority to one of eight options: 0 through 7.
- **Error Detect Timeout** – Provides a drop-down box you can use to set the error detect timeout value by selecting one of five options: 1 to 5 seconds. The default is one second.
- **Resource Allocate Timeout** – Provides a drop-down box you can use to set the resource allocate timeout value to one of five options: 1 to 5 seconds. The default is one second.
- **FCIP Timestamp** – Provides a drop-down box you can use to enable or disable FCIP timestamps. The default is enabled.
- **FCIP SW Compression** – Provides a drop-down box you can use to enable or disable FCIP compression. The default is disabled.
- **Bandwidth (Mbit/sec)** – Use this field to define the maximum bandwidth (in megabits per second) the GigE port will use during transmits. The range of values supported is 1 to 1000 megabits per second. Use this setting to limit the bandwidth used by the FCIP route so it doesn't consume all the available link bandwidth. For example, if the slowest link in the WAN being used is a DS-3 link, then the maximum available bandwidth is 45 megabits per second. To limit the FCIP route to 33% of the overall link bandwidth, set the bandwidth to 15 megabits per second.

NOTE:

To apply any changes made to this screen, click the **Save** button, located at the bottom of window.

FCIP Route Statistics Tabbed Page

The Statistics tabbed page consists of a scrollable table of parameters and values.

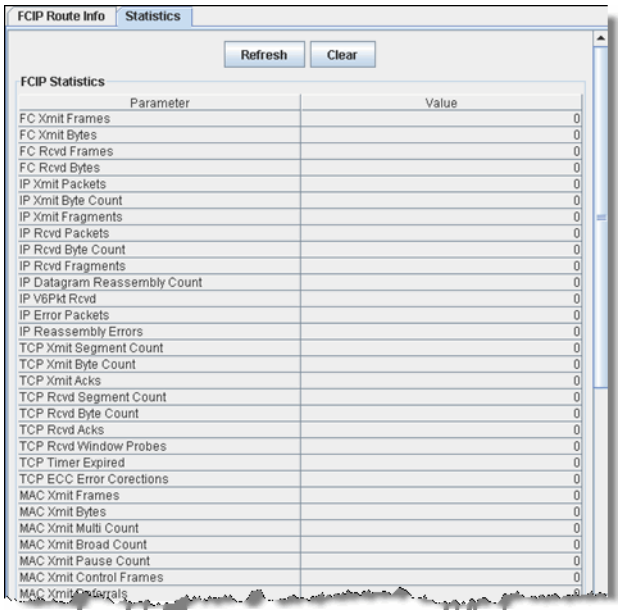


Figure 7-34 FCIP Route Statistics Page

You can refresh the statistics are by clicking **Refresh** at the top of the scrollable window. You can clear the statistics (set all values to zero) by clicking **Clear**.

Wizards

The SANsurfer iSCSI/FC Router Manager provides easy-to-use wizards that walk you through various router configuration procedures. You can launch an available wizard using any of the following methods:

- Select an option from the **Wizards** menu, located on the Router Manager's menu bar (see page 7-5.)
- Right-click anywhere within the router's node in tree window and select one of the wizards available from the action menu (see page 7-8.)
- If the router manager identifies unconfigured ports when you first connect to a router, it automatically launches the configuration wizard.

The following topics describe how to use the available wizards:

- Configuration Wizard (see page 7-44)
- Add Initiator Wizard (see page 7-49)
- FW Update Wizard (see page 7-51)
- Map Local Initiator/Target Wizard (see page 7-55)
- Unmap Local Initiator/Target Wizard (see page 7-63)
- Add Remote Router Wizard (see page 7-68)
- Remove Remote Router Wizard (see page 7-72)
- Map Remote Initiator/Target Wizard (see page 7-75)
- Remote Mapped Device (see page 7-81)
- Discover iSCSI Target Wizard (see page 7-84)
- FCIP Route Add Wizard (see page 7-86)
- FCIP Route Remove Wizard (see page 7-92)

Configuration Wizard

The Configuration Wizard provides a set of dialog boxes that walk you through the steps required for configuring the iSCSI ports. This wizard starts automatically when your system connects to a system with any un-configured iSCSI ports.

You can also start this wizard at any time by selecting **Configuration Wizard** from the **Wizards** menu or from the **Action Menu.**

After launching the Configuration Wizard, it displays the **iSCSI Port Selection** dialog box (see Figure 7-35).

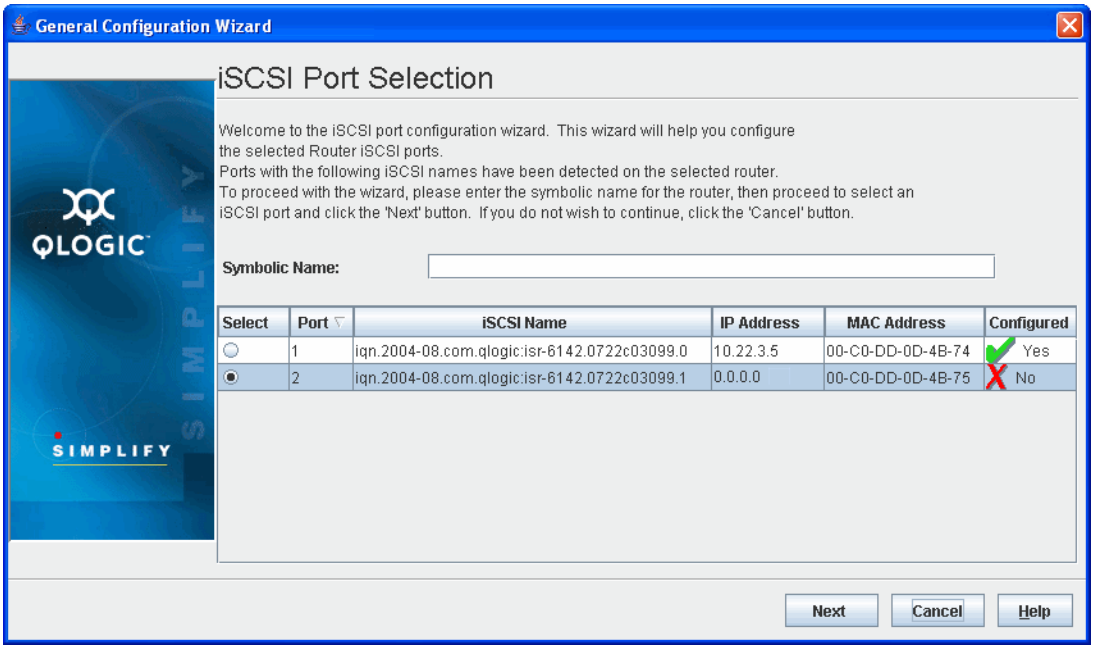


Figure 7-35 iSCSI Port Selection Dialog Box

To use the Configuration Wizard, follow these steps:

1. On the iSCSI Port Selection dialog box, select an unconfigured iSCSI port, enter the symbolic name for the router (if desired), then click **Next**.

   The **iSCSI Port Connection Settings Panel** dialog box displays (see Figure 7-36).

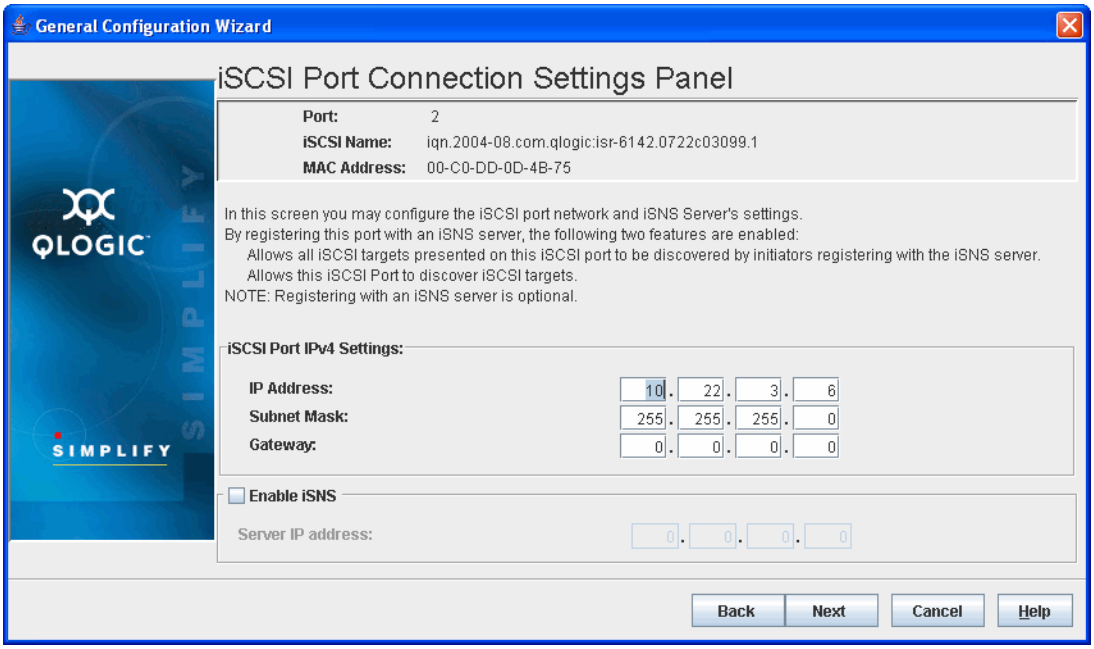

General Configuration Wizard
iSCSI Port Connection Settings Panel
Port: 2
iSCSI Name: iqn.2004-08.com.qlogic:isr-6142.0722c03099.1
MAC Address: 00-C0-DD-0D-4B-75
In this screen you may configure the iSCSI port network and iSNS Server's settings.
By registering this port with an iSNS server, the following two features are enabled:
Allows all iSCSI targets presented on this iSCSI port to be discovered by initiators registering with the iSNS server.
Allows this iSCSI Port to discover iSCSI targets.
NOTE: Registering with an iSNS server is optional.
iSCSI Port IPv4 Settings:
IP Address: 10 . 22 . 3 . 6
Subnet Mask: 255 . 255 . 255 . 0
Gateway: 0 . 0 . 0 . 0
Enable iSNS
Server IP address: 0 . 0 . 0 . 0
QLOGIC
SIMPLIFY
Back
Next
Cancel
Help

Figure 7-36 iSCSI Port Connection Settings Panel Dialog Box

2. To configure the iSCSI Port IPV4 settings:
   a. Type the information in the following fields.
      - **IP Address**
      - **Subnet Mask**
      - **Gateway**
   b. If desired, configure the IP address of the iSNS server with which the router registers the selected iSCSI port:
      - Select the **Enable iSNS** check box to make the **Server IP address** field editable.
      - Enter the IP address of the iSNS server in the **Server IP address** field.
3. Click **Next**. The **iSCSI Port IPv6 Settings Panel** appears, as shown in **Figure 7-37**.

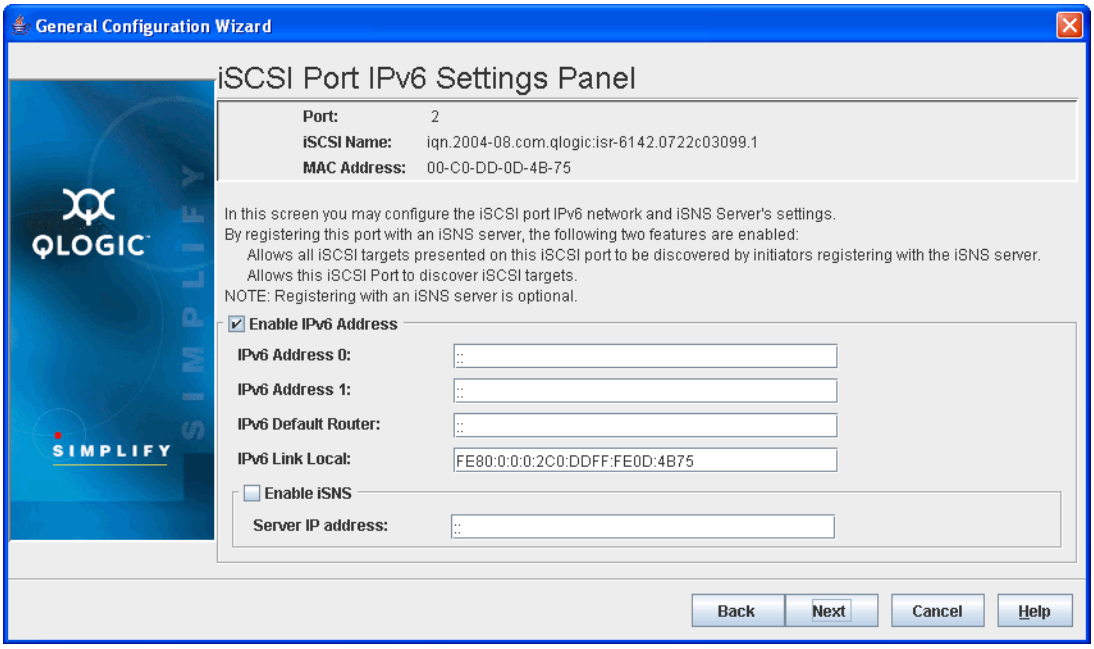

General Configuration Wizard
iSCSI Port IPv6 Settings Panel
Port: 2
iSCSI Name: iqn.2004-08.com.qlogic:isr-6142.0722c03099.1
MAC Address: 00-C0-DD-0D-4B-75
In this screen you may configure the iSCSI port IPv6 network and iSNS Server's settings.
By registering this port with an iSNS server, the following two features are enabled:
Allows all iSCSI targets presented on this iSCSI port to be discovered by initiators registering with the iSNS server.
Allows this iSCSI Port to discover iSCSI targets.
NOTE: Registering with an iSNS server is optional.
Enable IPv6 Address
IPv6 Address 0:
IPv6 Address 1:
IPv6 Default Router:
IPv6 Link Local:
FE80:0:0:0:2C0:DDFF:FE0D:4B75
Enable iSNS
Server IP address:
Back
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 7-37 iSCSI Port IPv6 Settings Panel

4. To configure the iSCSI port IPv6 connection using this dialog box, follow these steps:
   a. Select **Enable IPv6 Address** to make the fields editable.
   b. Specify the iSCSI port IPv6 network settings:
      - Enter the **IPv6 Address 0**.
      - Enter the **IPv6 Address 1**.
      - Enter the **IPv6 Default Router**.
      - Enter the **IPv6 Link Local**.
   c. If desired, configure the IP address of the iSNS server with which the router registers the selected iSCSI port:
      - Select the **Enable iSNS** check box to make the **Server IP address** field editable.
      - Enter the IP address of the iSNS server in the **Server IP address** field.
5. Click **Next**. The Confirm Changes dialog box displays, as shown in Figure 7-38.

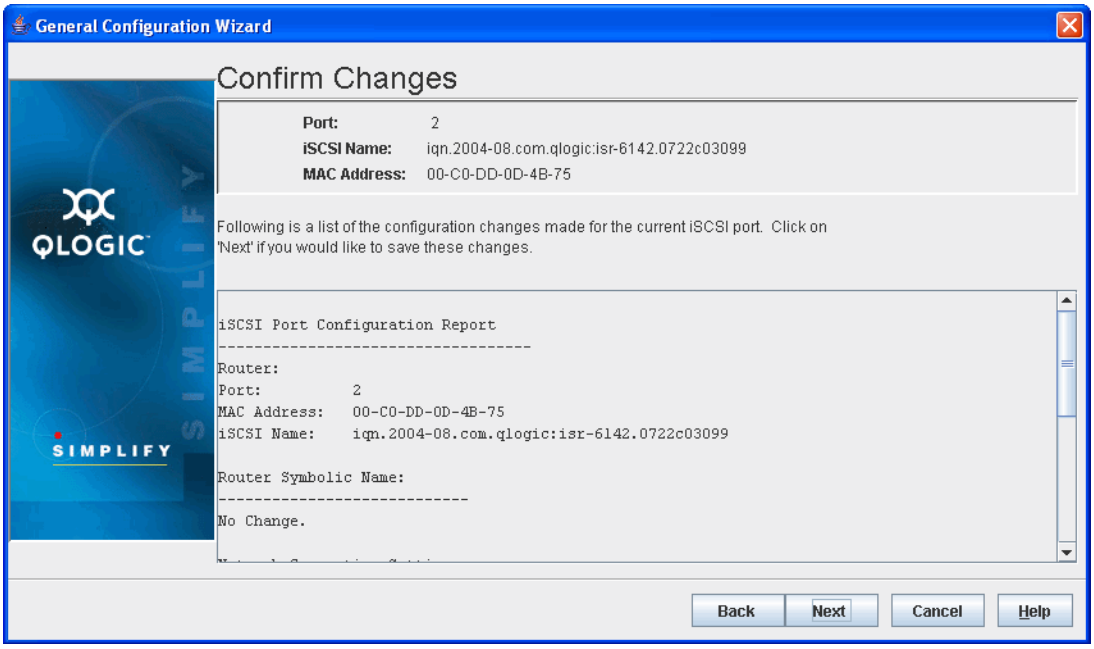


Figure 7-38 Confirm Changes Dialog Box

6. Review the configuration changes displayed on the screen, then click **Next** to confirm your changes.

The system displays the **iSCSI Port Configuration Status** dialog box, as shown in Figure 7-39.

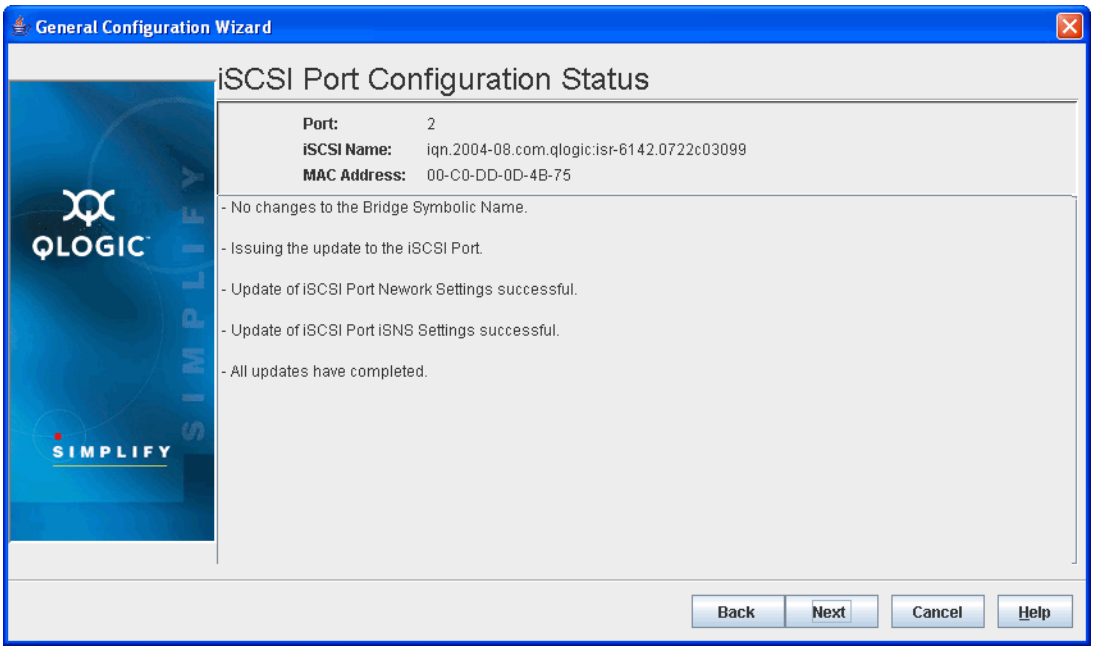


Figure 7-39 iSCSI Port Configuration Status

7. Read the information about the status changes, then click **Next**.

   The system displays the **Refresh** dialog box.

8. Read the information. If you would like to see the new configuration, click **Yes**; otherwise, click **No**.

   The system displays the **Finish** dialog box, as shown in Figure 7-40.

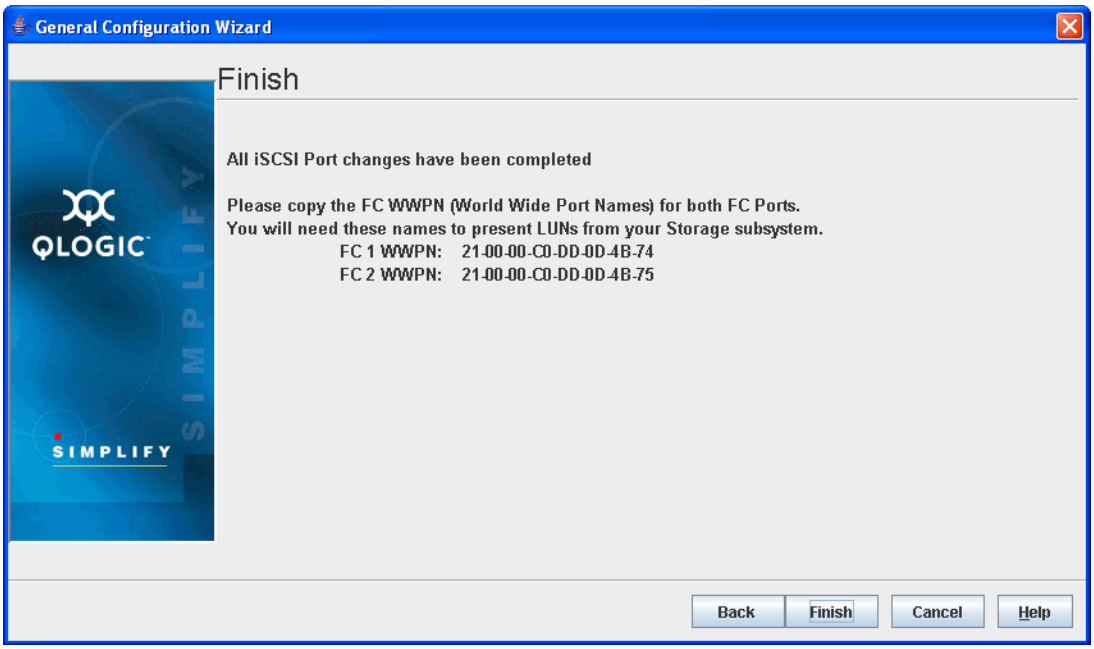


Figure 7-40 Configuration Wizard Finish Dialog Box

9. Read the information, then click **Finish**.

Add Initiator Wizard

The Add Initiator Wizard provides a dialog box used to enter an iSCSI initiator into the system database. iSCSI initiators are normally discovered (their name and address are captured) the first time they log in to the SANbox 6142 router.

This wizard allows you to enter the initiator information before the log in, thus allowing you to map LUNs to the initiator before logging into the SANbox 6142.

You can also start this wizard at any time by selecting **Add Initiator Wizard** from the **Wizards Menu** or from the **Action Menu**.

After launching the Configuration Wizard, the system displays the **iSCSI Port Selection** dialog box, as shown in Figure 7-41.

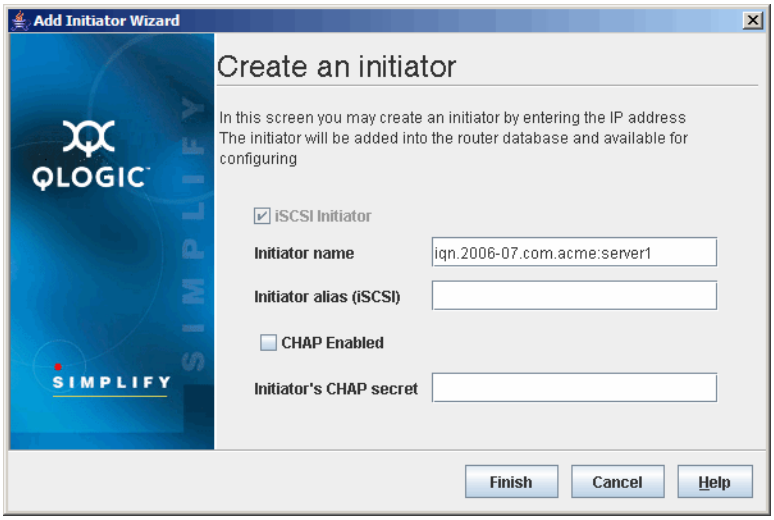


Figure 7-41 Create an Initiator Dialog Box

To create an initiator:

1. Type a name in the **Initiator name** box.
2. Type an alias in the **Initiator alias (iSCSI)** box.
3. If you want to enable CHAP for this initiator, select the **CHAP Enabled** check box. If you want a CHAP secret, type the name in the Initiator's **CHAP Secret** box.
4. Click **Finish**. The **Security Check** dialog box displays, as shown in Figure 7-42.

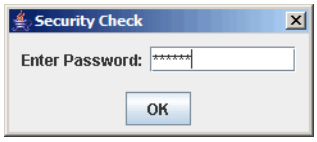


Figure 7-42 Security Check Dialog Box

5. Type the appropriate password, then click **OK**.

The new iSCSI initiator is displayed in the discovered iSCSI initiator's section of the system tree, as shown in Figure 7-43.

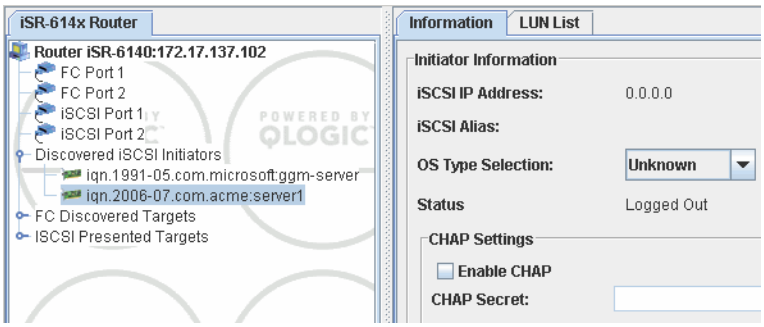


Figure 7-43 System Tree with New iSCSI Initiator

FW Update Wizard

The FW Update Wizard provides a set of dialog boxes that walk you through the steps required for updating the SANbox 6142 firmware. This wizard helps you update the firmware on selected router. When you first launch this wizard, the Router Selection dialog box displays all detected routers, as shown in Figure 7-44.

You can start this wizard at any time by selecting **FW Update Wizard** from the **Wizards Menu** or from the **Action Menu**.

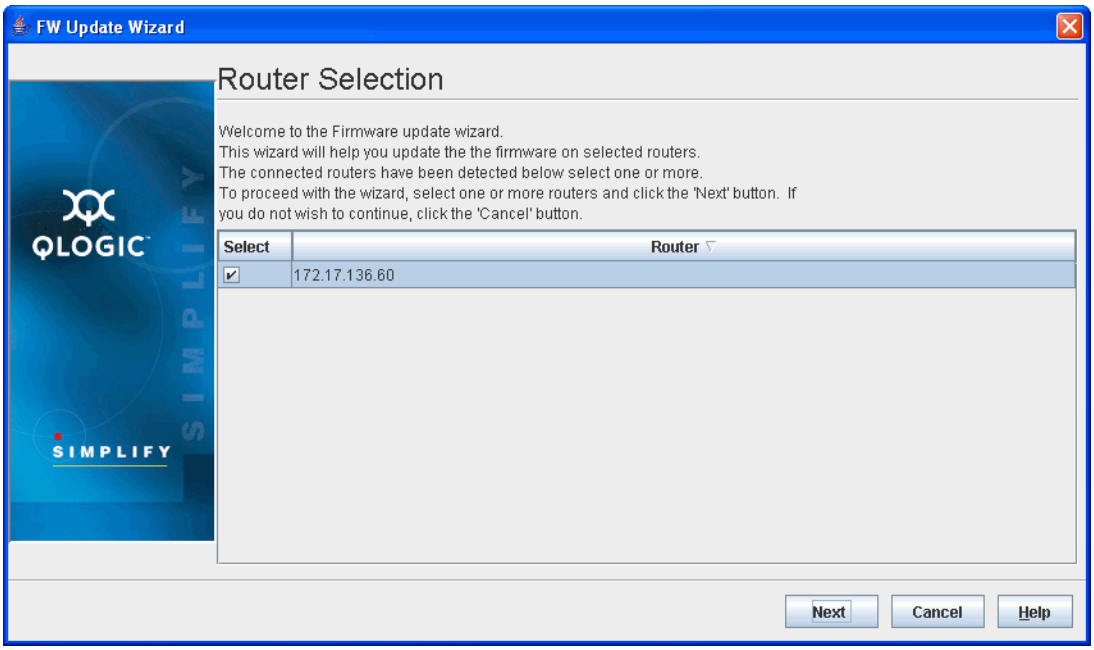

FW Update Wizard
Router Selection
Welcome to the Firmware update wizard.
This wizard will help you update the the firmware on selected routers.
The connected routers have been detected below select one or more.
To proceed with the wizard, select one or more routers and click the 'Next' button. If you do not wish to continue, click the 'Cancel' button.
Select
Router
172.17.136.60
SIMPLIFY
Next
Cancel
Help

Figure 7-44 Router Selection Dialog Box

To update the firmware, follow these steps:

1. Select the check box next to the routers whose firmware you want to update, then click **Next**. The **Open** dialog box displays.

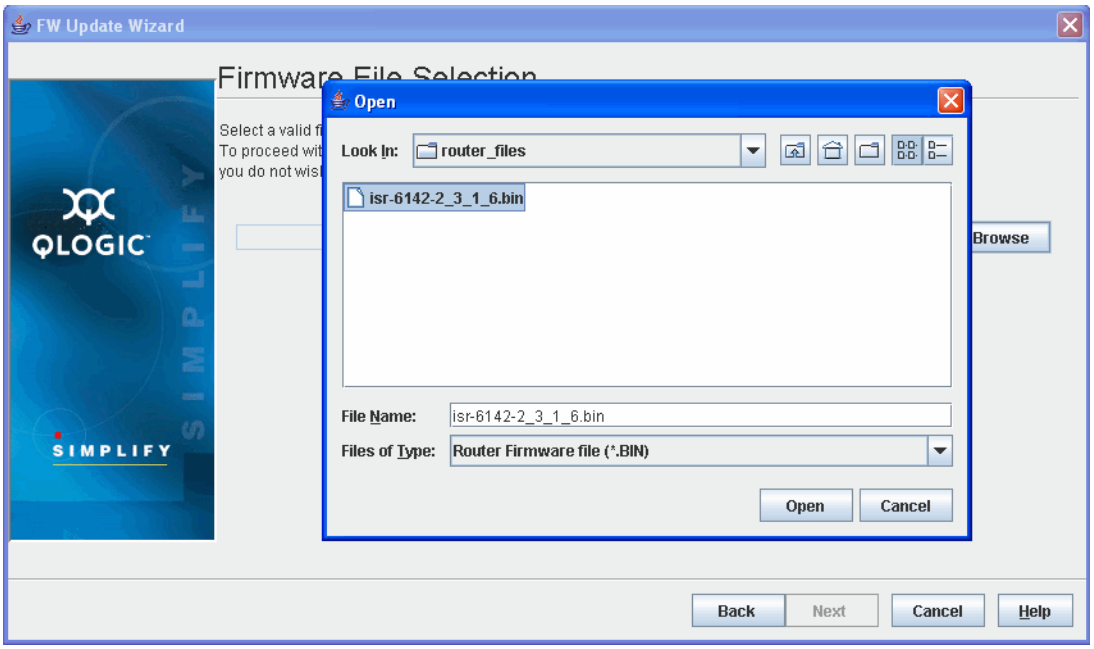


Figure 7-45 Firmware File Selection Dialog Box

2. Enter in the path to the firmware file, or click **Browse** to locate the firmware file.
3. When the firmware file is displayed in the **Firmware Image File** field, click **Next**.

The **Confirm Changes** dialog box displays, as shown in Figure 7-46.

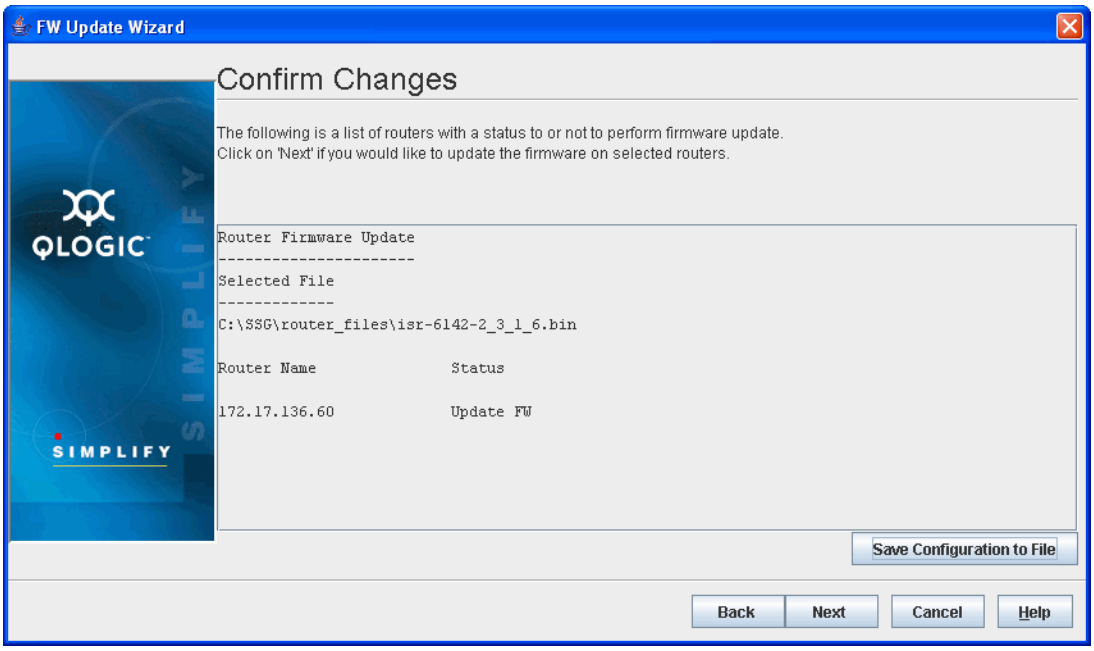


Figure 7-46 Confirm Changes Dialog Box

4. Read the information, then do the following:
   a. If you want to save a copy of this firmware configuration, click **Save Configuration to File**. Browse to the desired directory, type a file name, then click **Save**.
   b. Click **Next**. The **Security Check** dialog box requests the Admin password, as shown in Figure 7-47.

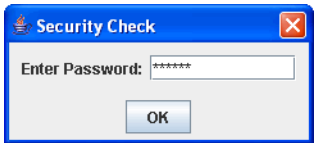


Figure 7-47 Security Check Dialog Box

   c. Type the appropriate password, then click **OK** to start the firmware update.
5. The **Firmware Update Status** dialog box shows the progress of the update in the message section, as shown in Figure 7-48.

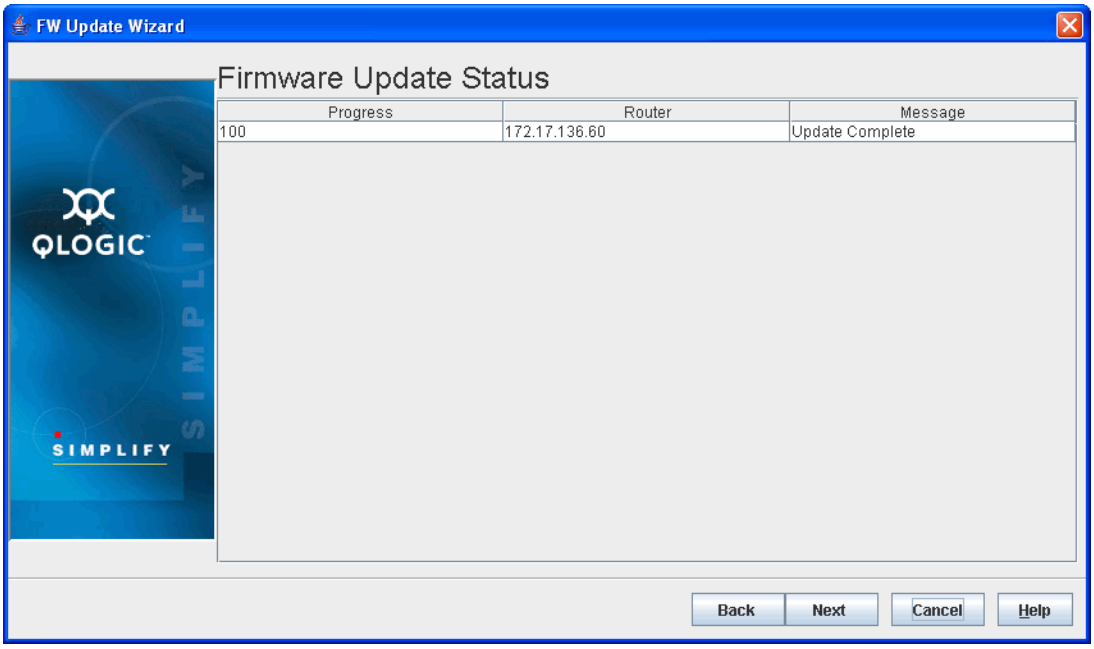


Figure 7-48 Firmware Update Status Dialog Box—Progress

When the firmware has loaded successfully, the system displays the **Finish** dialog box, along with the **Update success** dialog box, as shown in Figure 7-49.

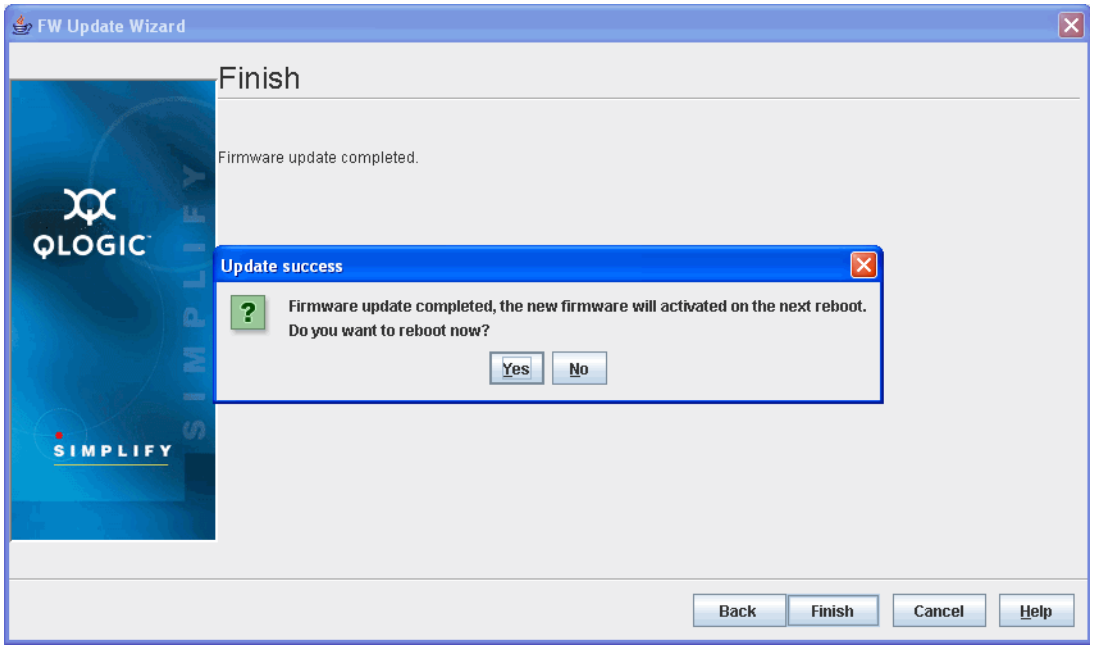


Figure 7-49 Finish Dialog Box (Successful Firmware Update)

NOTE:

The new firmware will not take effect until the system is rebooted.

6. Complete the wizard:
   a. If you want to reboot the system now, click **Yes**. Otherwise, click **No**.
   b. Click **Finish**.

Map Local Initiator/Target Wizard

The Map Local Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for mapping a local initiator to a local target.

You can start this wizard at any time by selecting **Map Local Initiator/Target Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the Map Local Initiator/Target wizard launches, the **Select an Initiator** dialog box displays a list of locally connected initiators (FC or iSCSI), as shown in Figure 7-50.

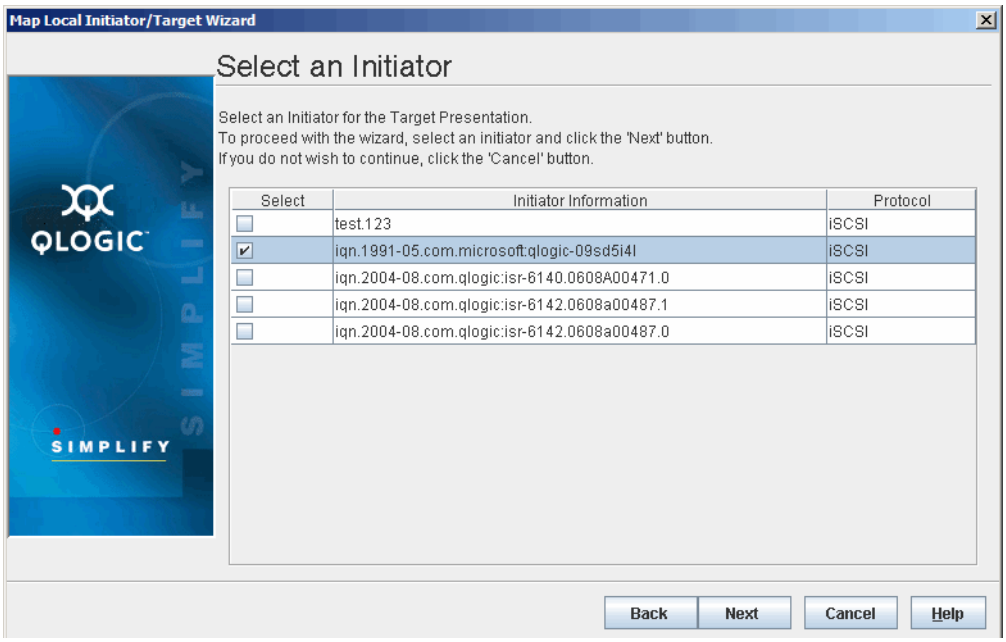


Figure 7-50 Initiator Selection Dialog Box

To map a local target to a local initiator:

1. Select the check box next to the initiator you want to map, then click **Next**.

The **Select a Target** dialog box opens, as shown in Figure 7-51.

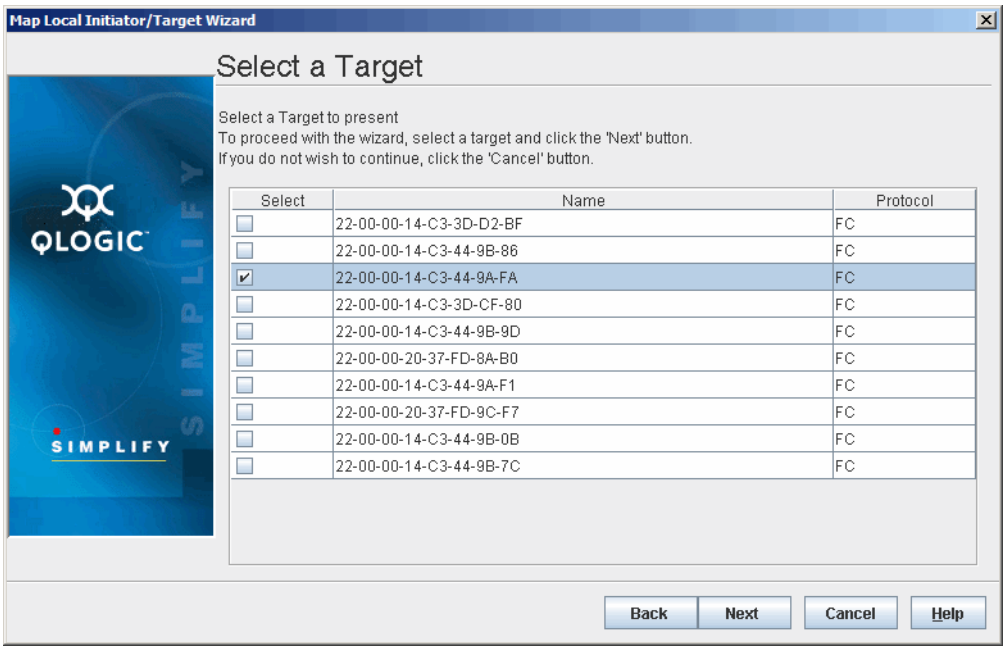


Figure 7-51 Select a Target Dialog Box

2. Select a target you want mapped to the previously selected initiator, then click **Next**.

The wizard screen prompts you to select a port on which the initiator will be presented, as shown in Figure 7-52.

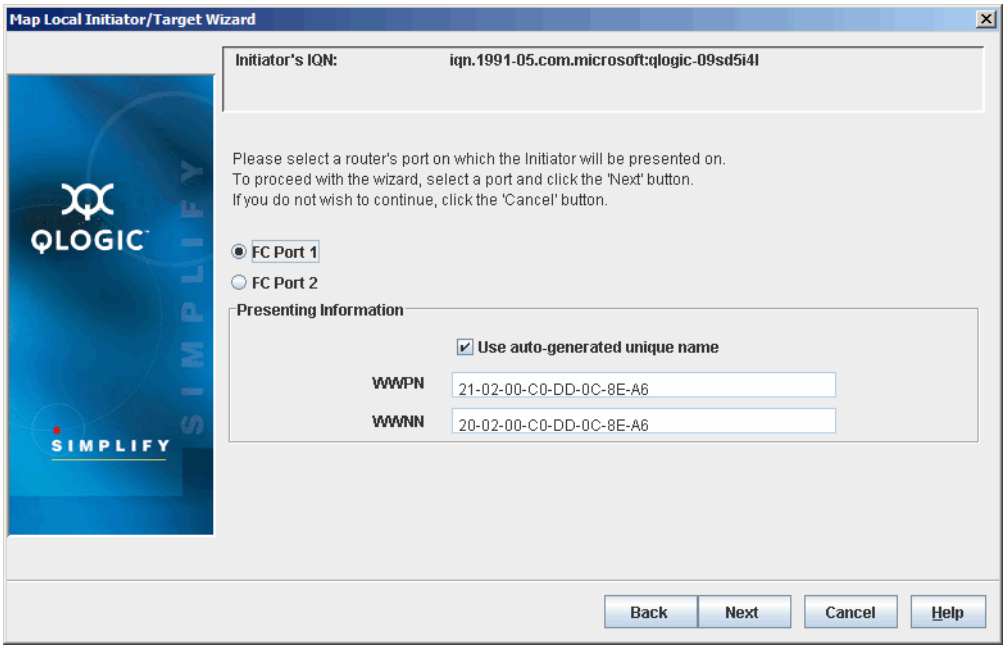


Figure 7-52 Select Initiator Port Dialog Box

3. Select the port (FC Port 1 or FC Port 2), then click **Next**.

The wizard screen prompts you to select a port on which the target will be presents (iSCSI Port 1 and iSCSI Port 2), as shown in Figure 7-53.

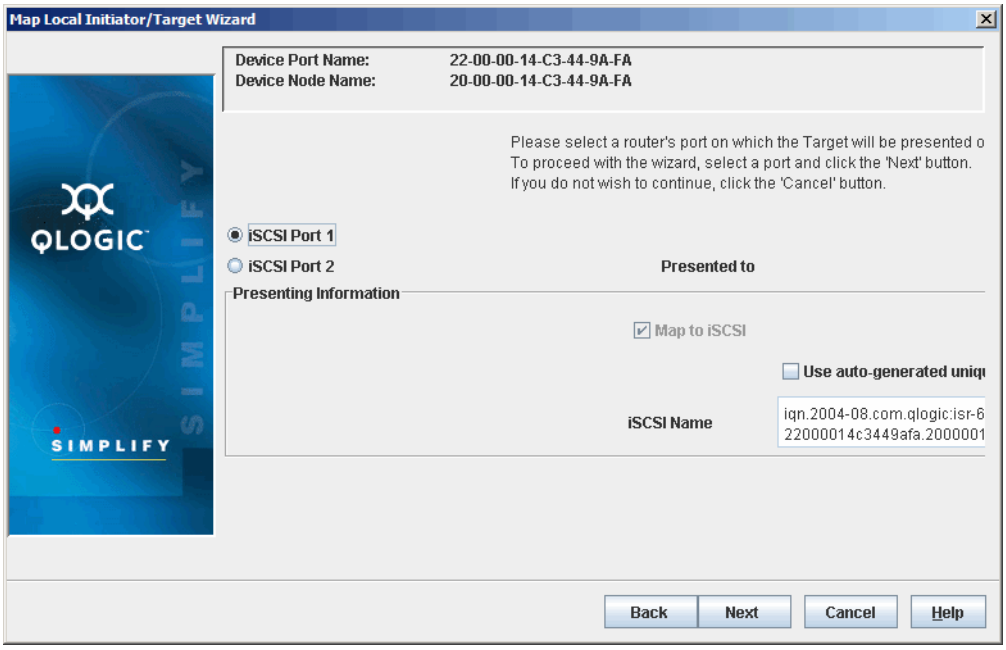


Figure 7-53 Select Target Presentation Port Dialog Box

The **Confirm Changes** dialog box displays the local mapping done in the previous steps, as shown in Figure 7-54.

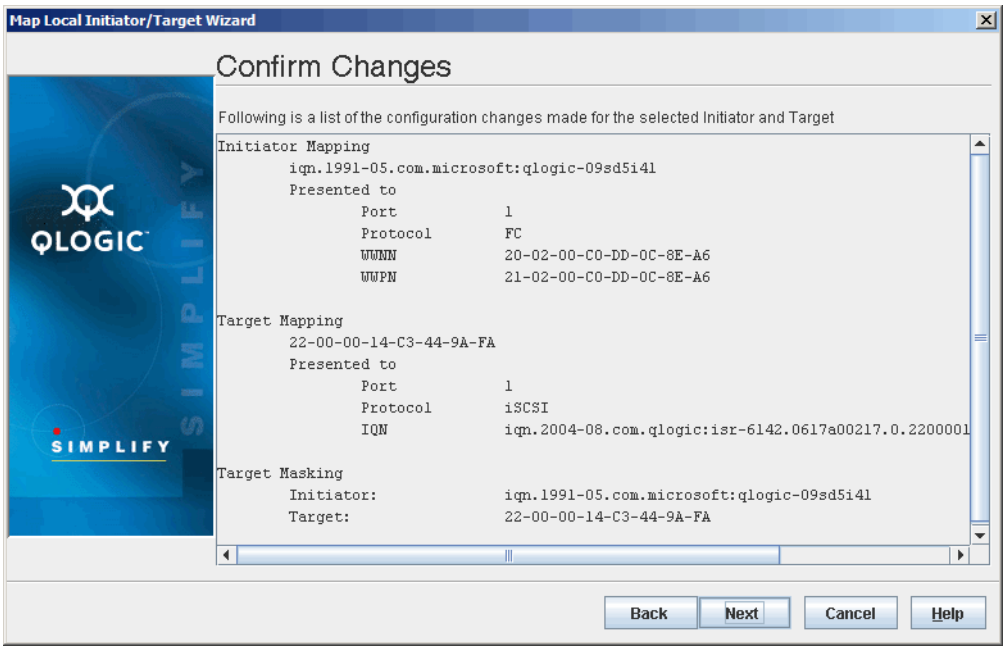


Figure 7-54 Confirm Changes Dialog Box

4. Review the information, then click **Next**.

The **Security Check** dialog box requests the Admin password, as shown in Figure 7-55.

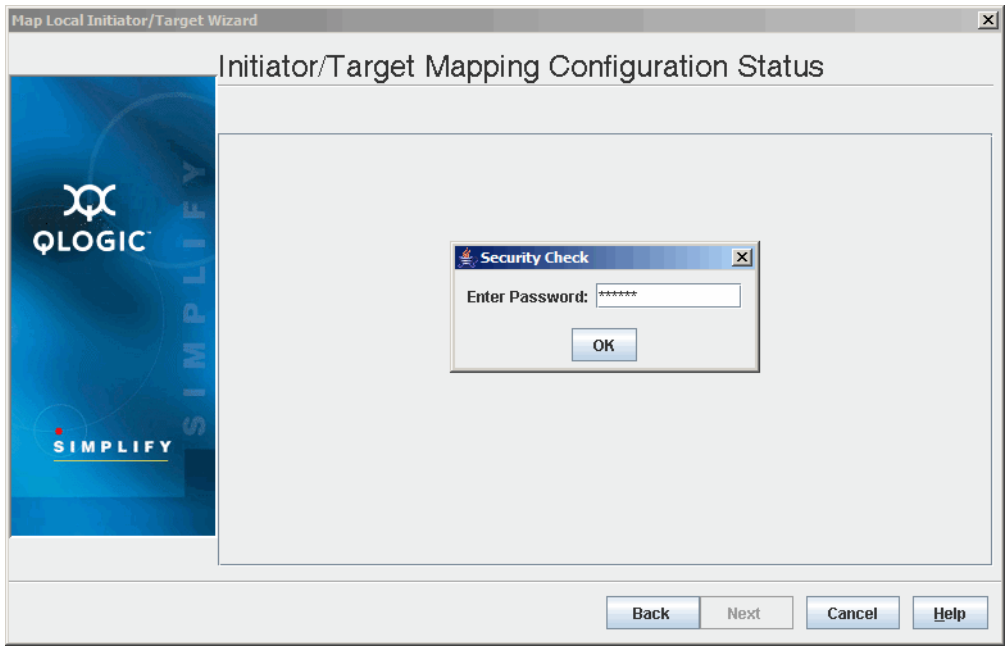


Figure 7-55 Security Check Dialog Box

5. Type the appropriate password, then click **OK** to confirm the local mapping.

The **Initiator/Target Mapping Configuration Status** dialog box displays local mapping completion status, as shown in Figure 7-56.

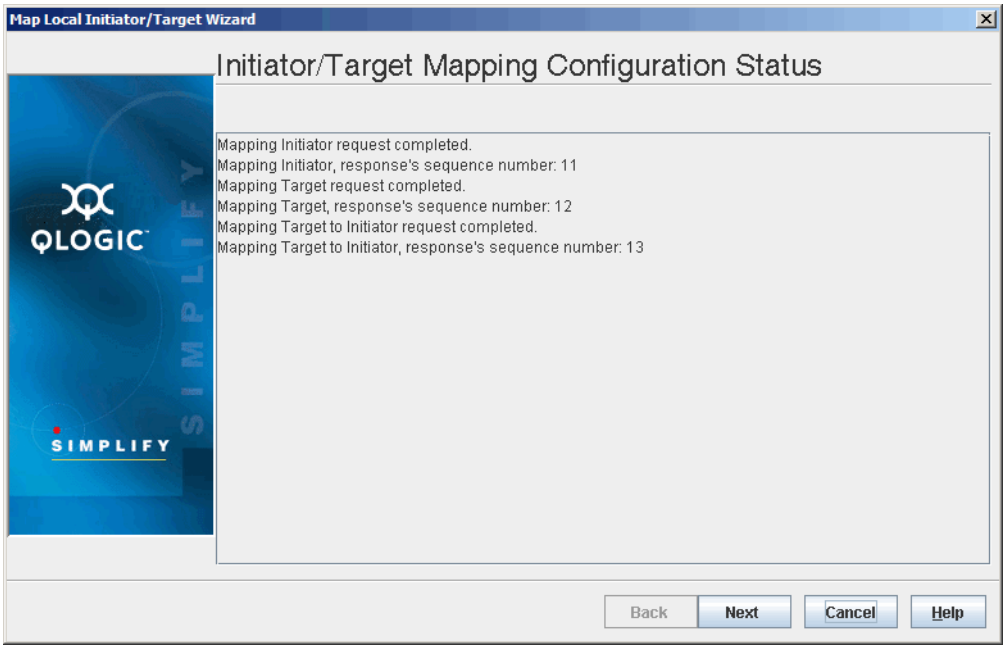


Figure 7-56 Initiator/Target Mapping Configuration Status Dialog Box

6. After reviewing the initiator to target mapping configuration status, click **Next**.

After completing the Map Local Initiator/Target wizard, you can see the mapping by selecting the mapped Initiator in the system tree under **Discovered iSCSI Initiators**. Click the **Local Presented Devices** tab, as shown in Figure 7-57. In this example an iSCSI initiator is mapped to an FC target, other mappings are supported such as FC to FC, FC to iSCSI and iSCSI to iSCSI.

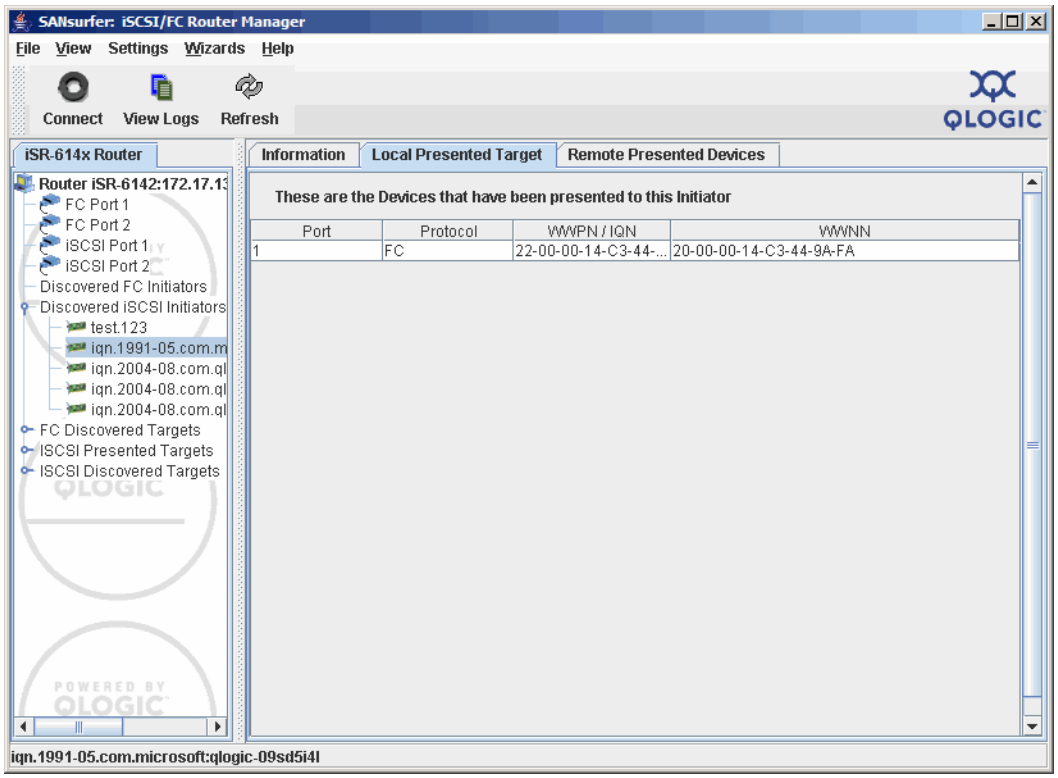


Figure 7-57 Discovered iSCSI Initiators - Local Presented Targets

Unmap Local Initiator/Target Wizard

The Unmap Local Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for removing a local initiator from a local target mapping.

You can start this wizard at any time by selecting **Unmap Local Initiator/Target Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the UnMap Local Initiator/Target wizard launches, the **Select an Initiator** dialog box displays a list of locally connected initiators (FC or iSCSI), as shown in Figure 7-58.

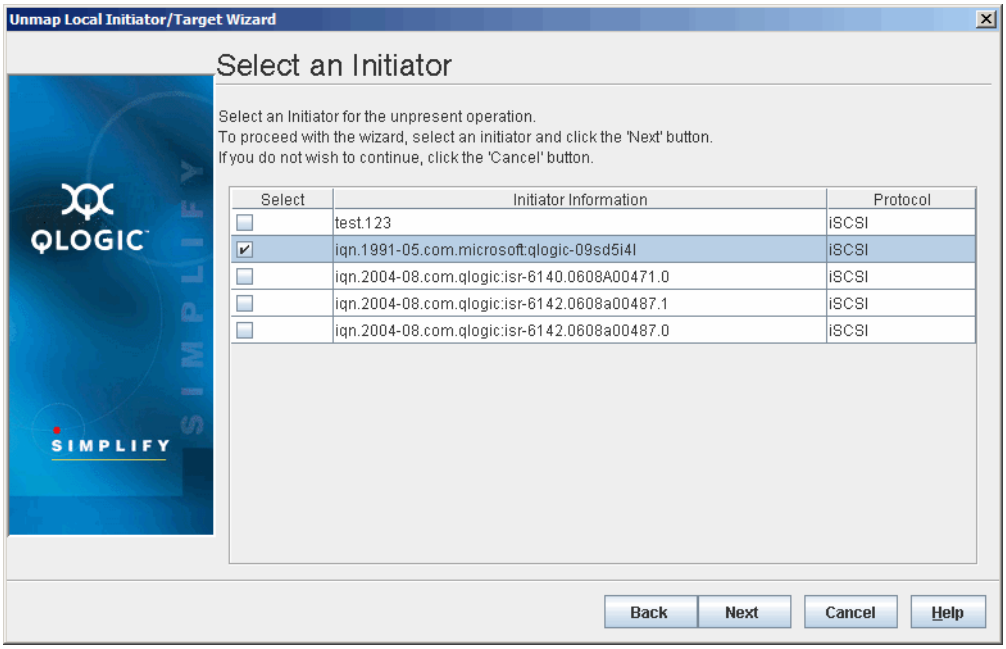


Figure 7-58 Initiator Selection Dialog Box

To unmap a local target from a local initiator:

1. Select the check box next to the initiator you want to unmap, then click **Next**.

The **Presented Target Selection** dialog box displays a list of targets mapped to the initiator selected in the previous step, as shown in Figure 7-59.

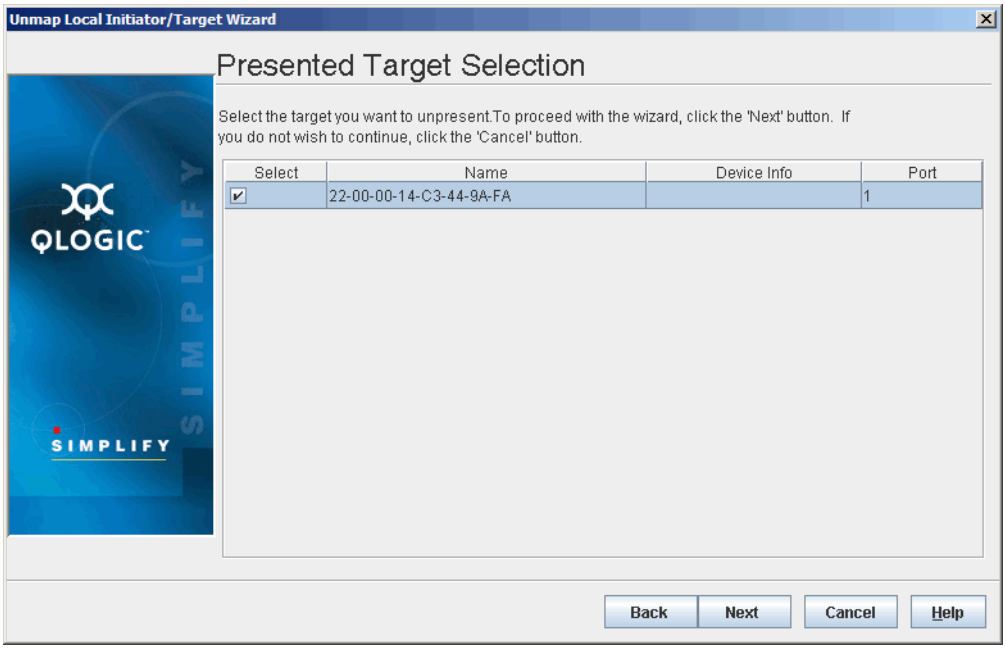


Figure 7-59 Presented Target Selection Dialog Box

2. Select the check box next to the target to unmap, then click **Next**.

The **Security Check** dialog box requests the Admin password, as shown in Figure 7-60.

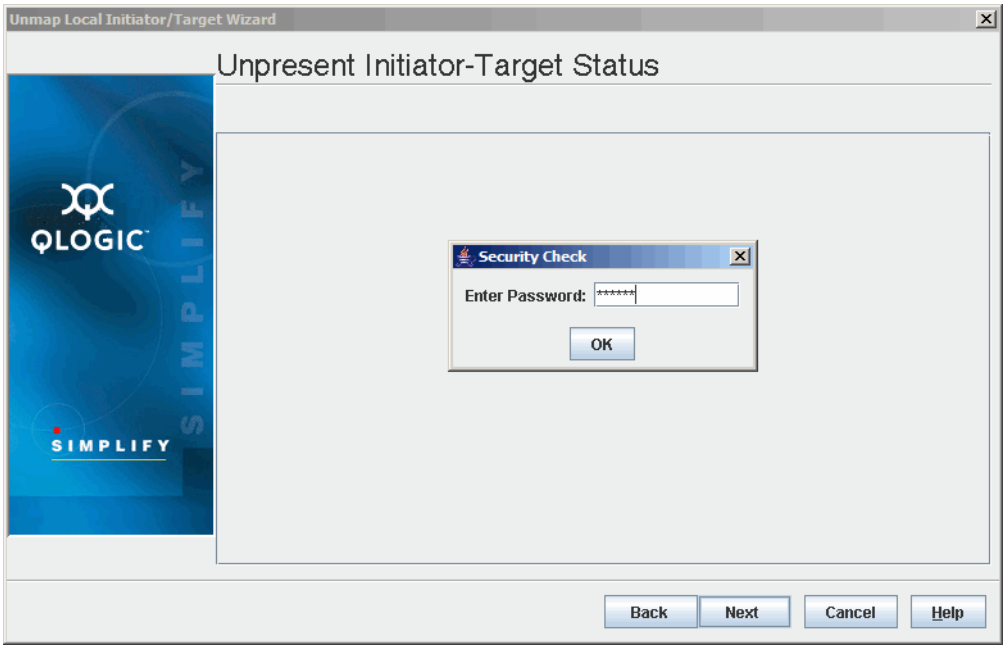


Figure 7-60 Security Check Dialog Box

3. Type the appropriate password, then click **OK** to confirm the target is unmapped.

The **Unpresent Initiator/Target Status** dialog box displays the results of the unmap operation, as shown in Figure 7-61.

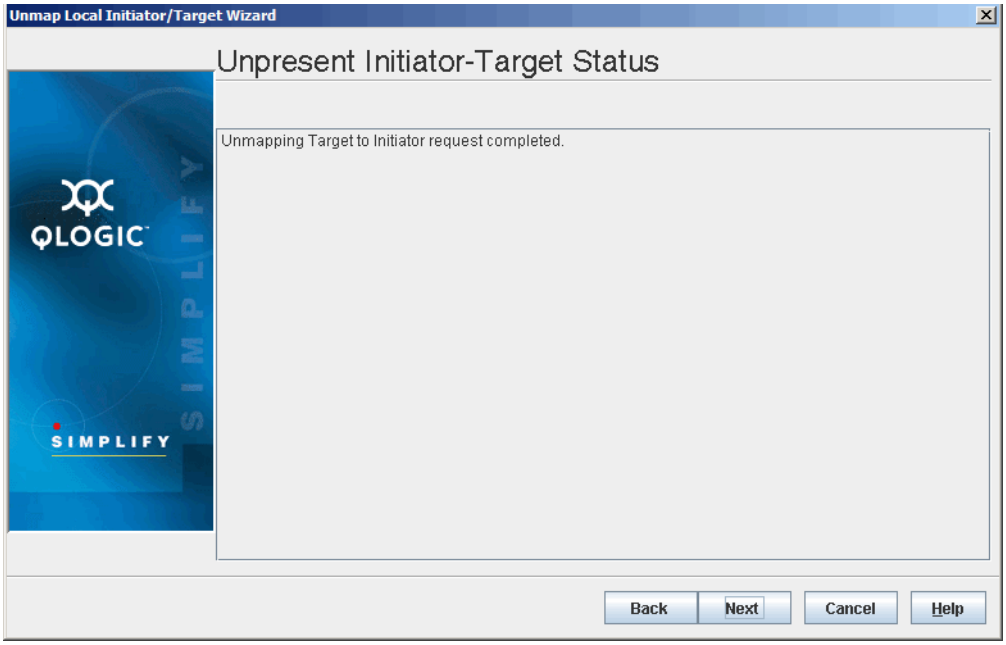


Figure 7-61 Unpresent Initiator/Target Status Dialog Box

4. Review the status, then click **Next**.

After completing the UnMap Local Initiator/Target wizard you can verify the unmapping by selecting the Initiator in the system tree under **Discovered iSCSI Initiators.** Then select **Local Presented Devices**.

For the example shown in Figure 7-62, an iSCSI initiator was unmapped from an FC target.

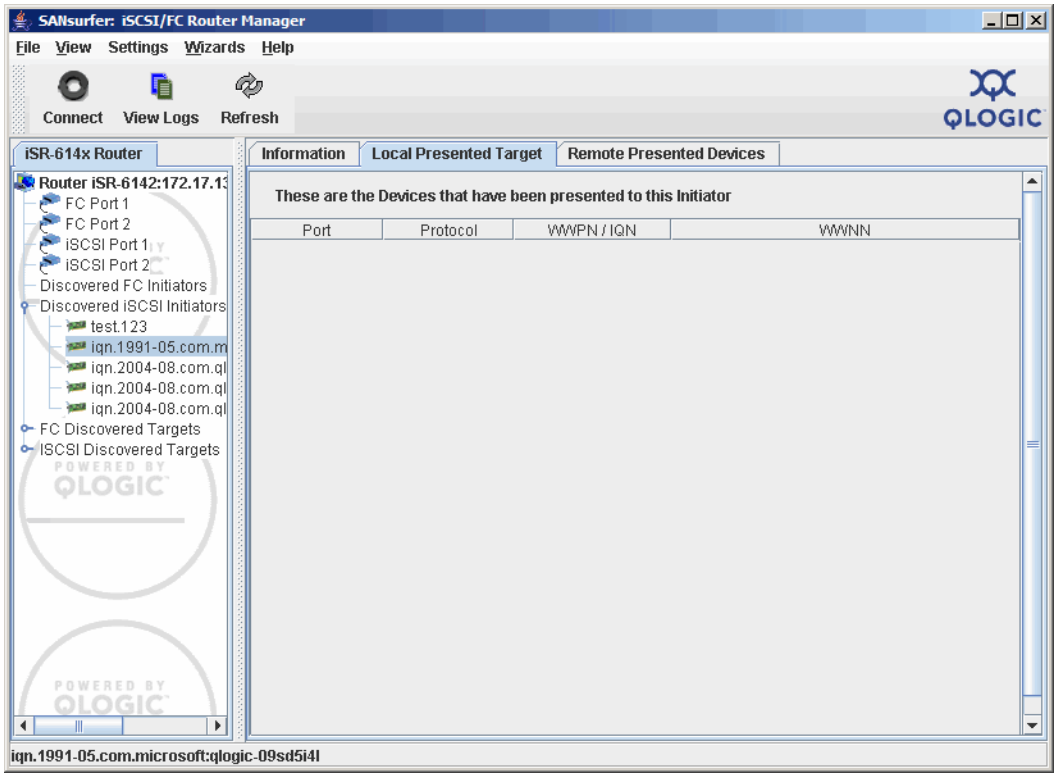


Figure 7-62 Discovered iSCSI Initiators - Local Presented Targets

Add Remote Router Wizard

The Add Remote Router Wizard provides a set of dialog boxes that walk you through the steps required for assigning a remote router to your local router as a peer.

You can start this wizard at any time by selecting **Add Remote Router Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the Add Remote Router wizard launches, the **Remote Router's IP Address** dialog box requests the remote router's IP address, as shown in Figure 7-63.

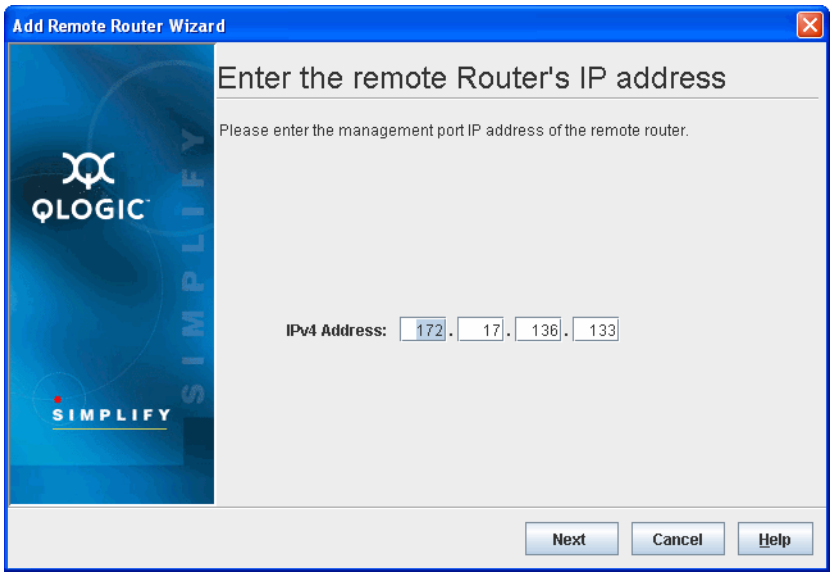


Figure 7-63 Remote Router's IP Address Dialog Box

To add a remoter router to a local router:

1. Type the IP Address of the remote router, then click **Next**.

The **Status** dialog box displays the remote router information along with the **Local Router Admin Password** dialog box, as shown in Figure 7-64.

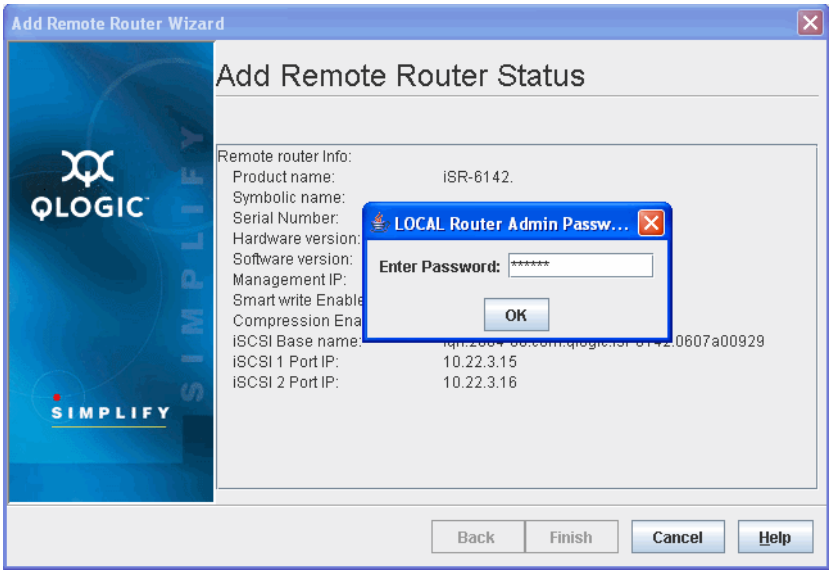


Figure 7-64 Local Router Admin Password Dialog Box

2. Type the local router admin password (default=config), then click **OK**.

   The **Status** dialog box displays the remote router information, as shown in Figure 7-65.

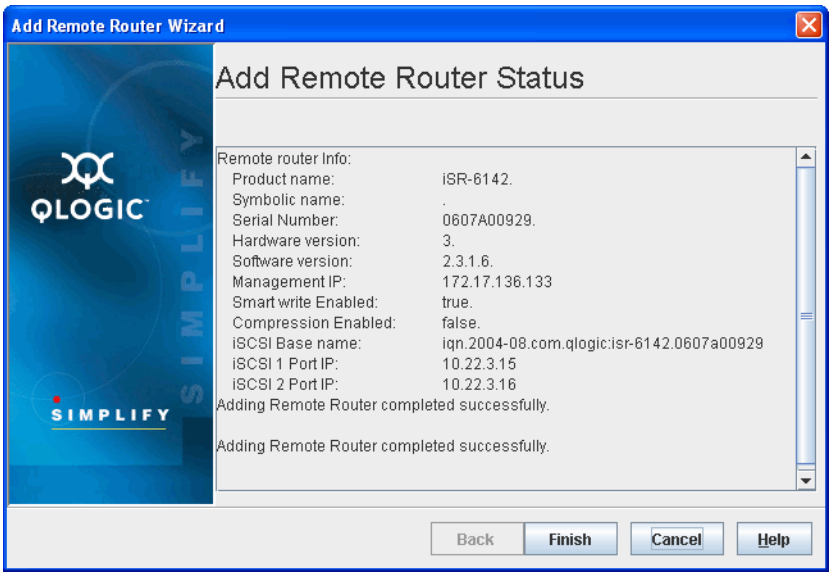


Figure 7-65 Add Remote Router Status Dialog Box

3. Review the status, then click **Finish**.
4. Click the **Refresh** icon to refresh the display.
5. Select the router node, then select the **Assigned Remote Router:1** tab to display the remote router's information, as shown in Figure 7-66.

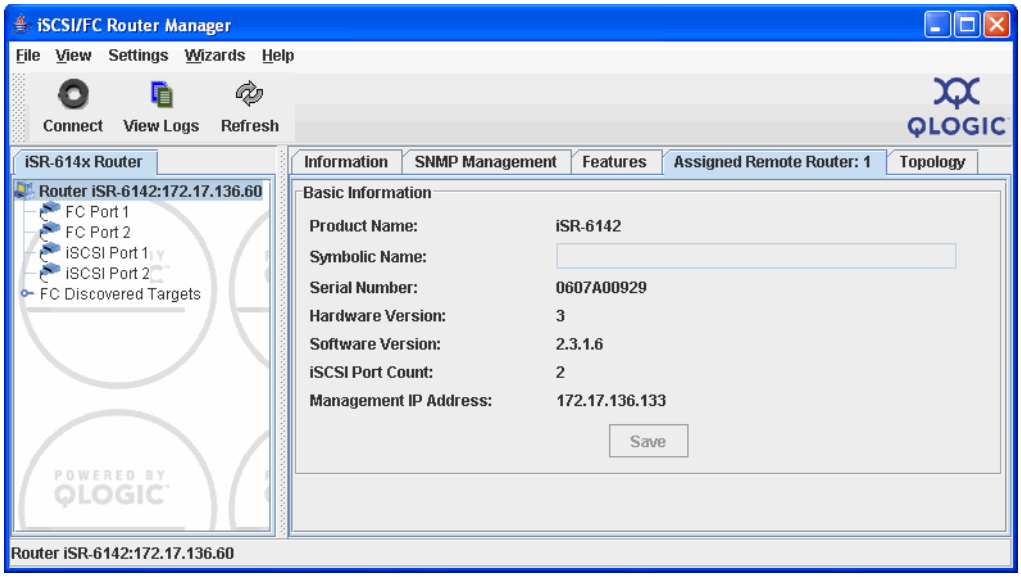


Figure 7-66 Assigned Remote Router Display

6. Click the **Topology** tab to display the local and remote router topology including devices attached to both routers, as shown in Figure 7-67.

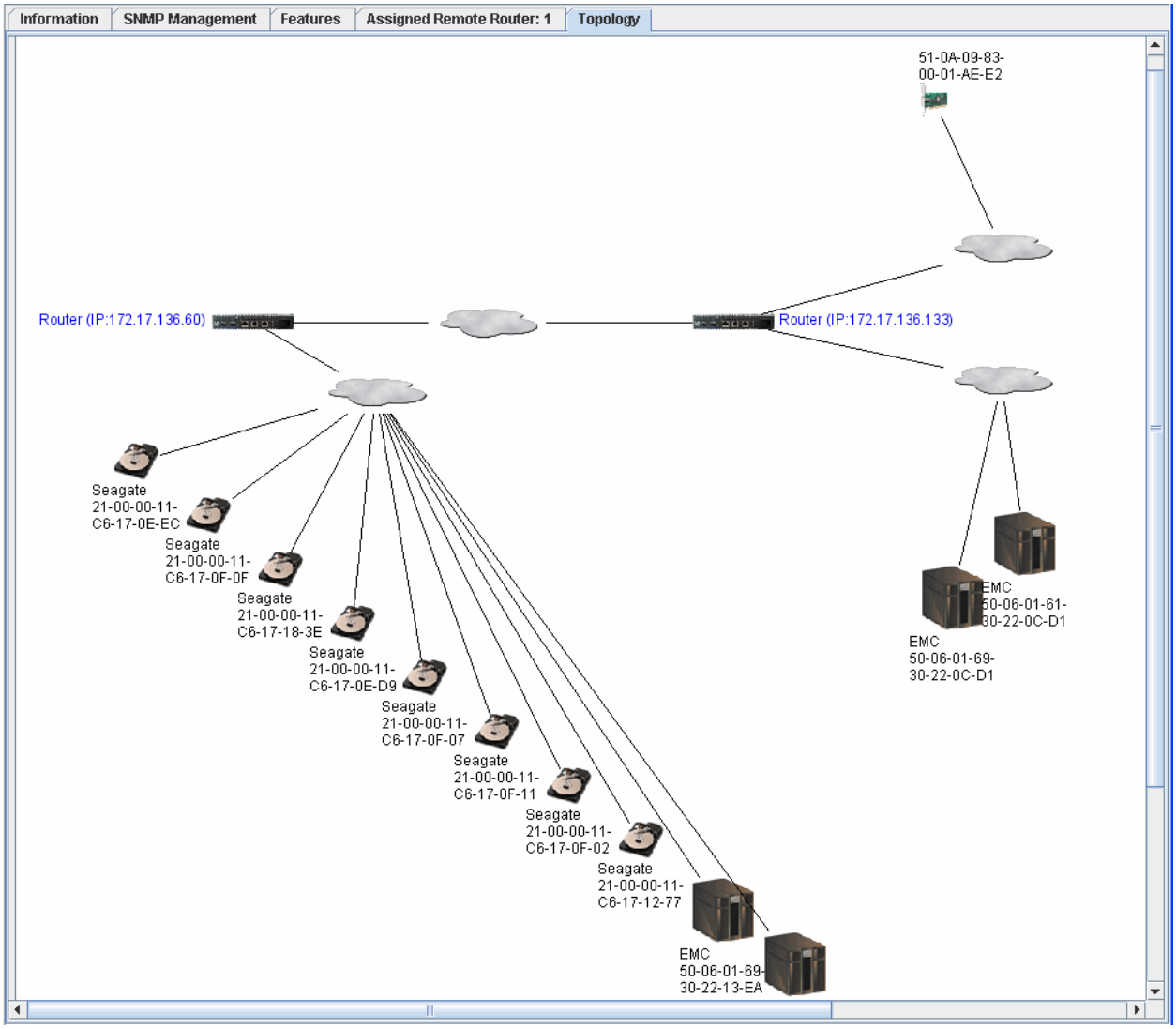


Figure 7-67 Topology Display

Remove Remote Router Wizard

The Remove Remote Router Wizard provides a set of dialog boxes that walk you through the steps required for removing a remote router from the local router.

You can start this wizard at any time by selecting **Remove Remote Router Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the Remove Remote Router wizard launches, the **Select a Remote Router to unmap** dialog box displays a list of mapped routers, as shown in Figure 7-68.

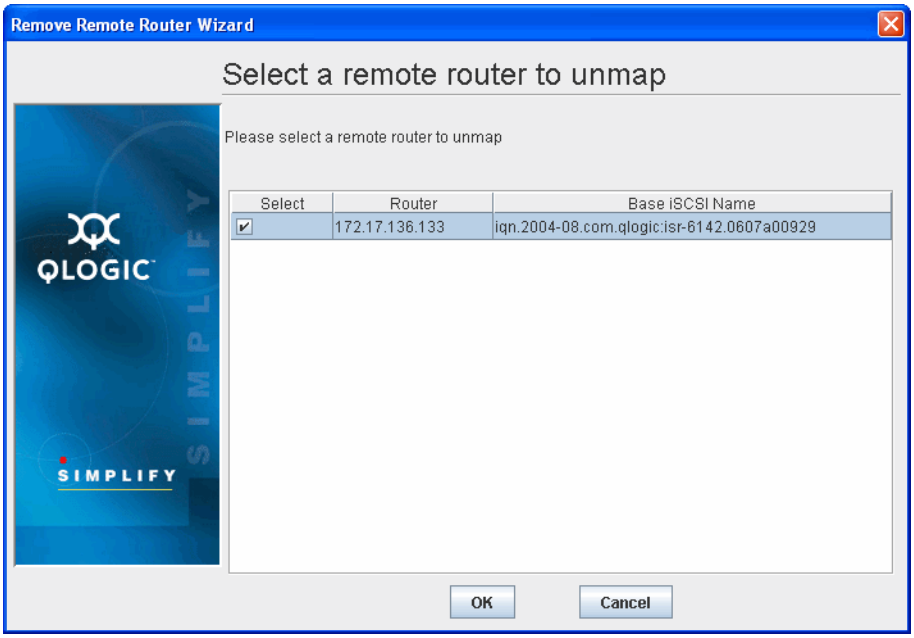


Figure 7-68 Select Remote Router Dialog Box

To remove a remoter router from a local router:

1. Select the remote router to be removed, then click **OK**.

The **Local Router Admin Password** dialog box requests the local router's admin password to complete the unmap, as shown in Figure 7-69.

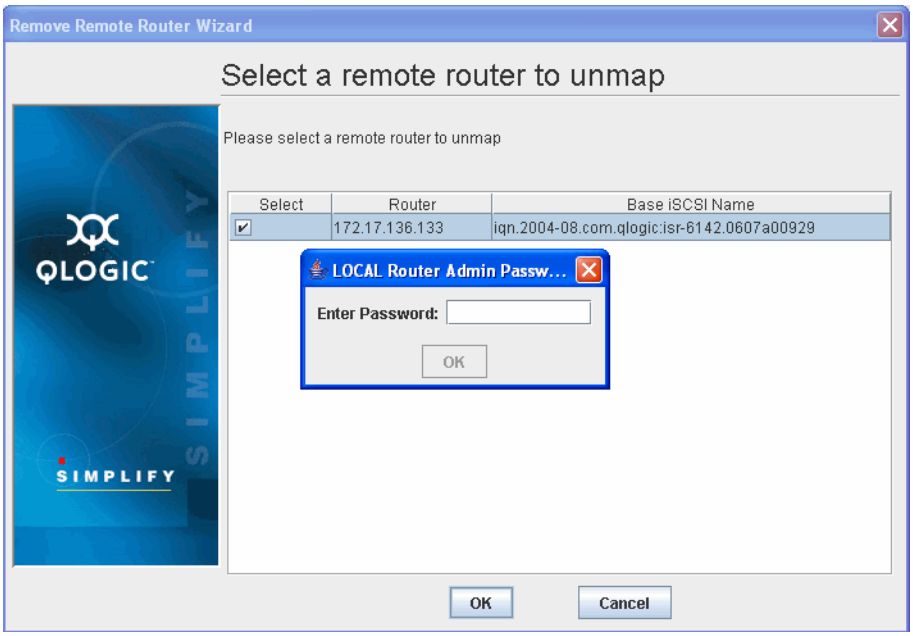


Figure 7-69 Local Router Admin Password Dialog Box

2. Type the local router's admin password (default=config), then click **OK**.

   The system prompts you to refresh the display, as shown in Figure 7-70.

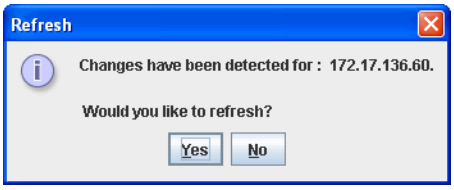


Figure 7-70 Refresh Screen

3. Click **Yes** to refresh the display.

The **Remove Remote Router Completion** dialog box displays the completion status, as shown in Figure 7-71.

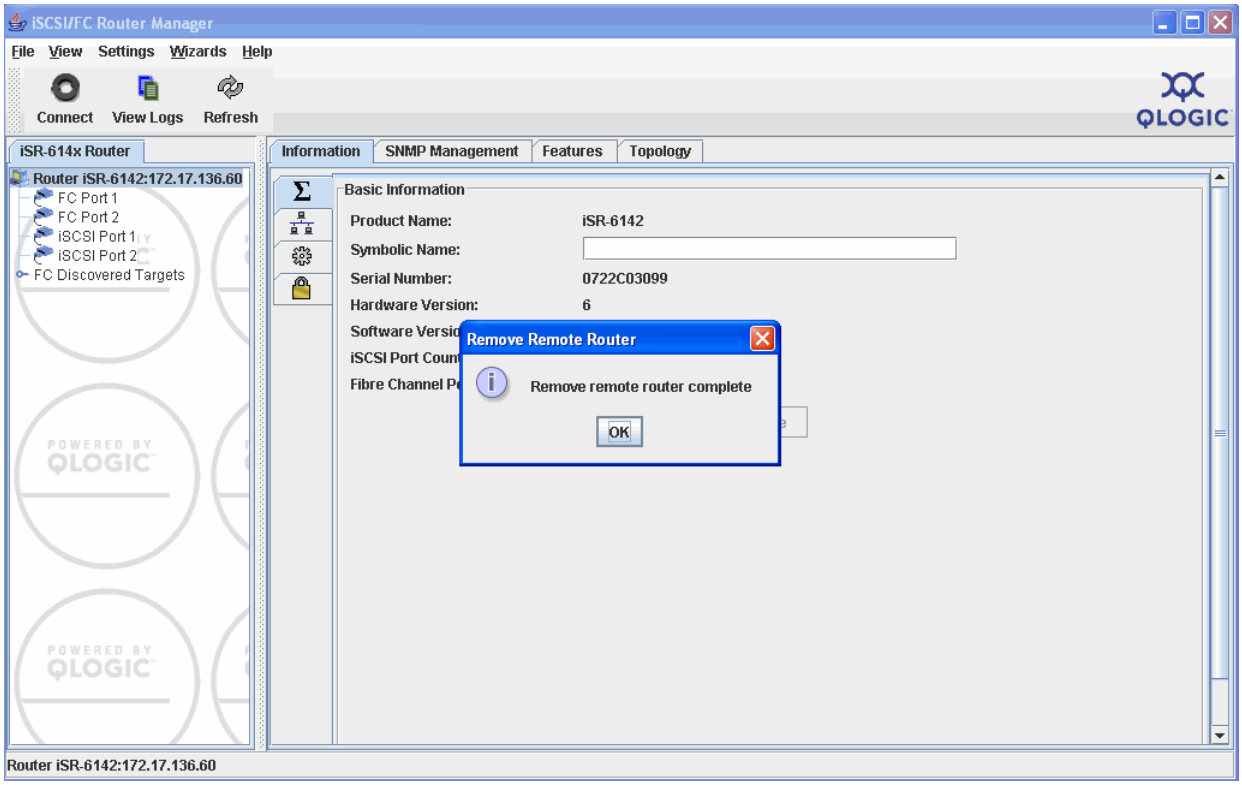


Figure 7-71 Remove Remote Router Completion Dialog Box

4. Click **OK** to close the message box.

Map Remote Initiator/Target Wizard

The Map Remote Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for mapping an initiator to a target one of which is remote and the other local.

You can start this wizard at any time by selecting **Map Remote Initiator/Target Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the Map Remote Initiator/Target wizard launches, the **Device Selection** dialog box displays a list of devices, as shown in Figure 7-72. If necessary, expand the router tree to see the attached devices.

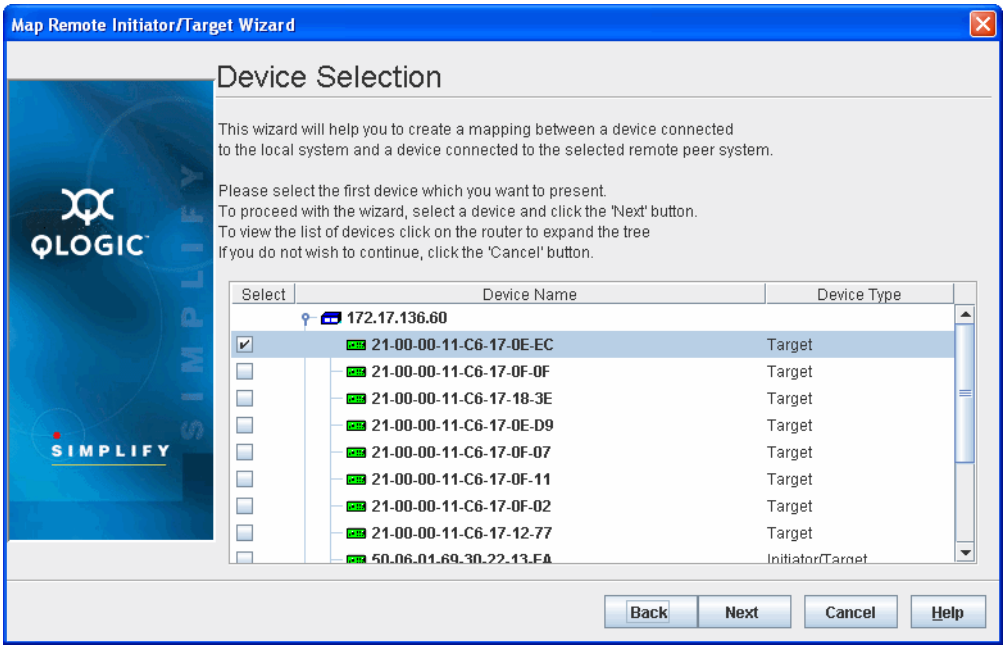


Figure 7-72 Device Selection Dialog Box

To create a remote-to-local mapping between an initiator to a target:

1. Select the device to be mapped. The device may be a target or an initiator and may be either on the remote router or on the local router.
2. Click **Next**.

The **Device Selection** dialog box displays list of devices, as shown in Figure 7-73.

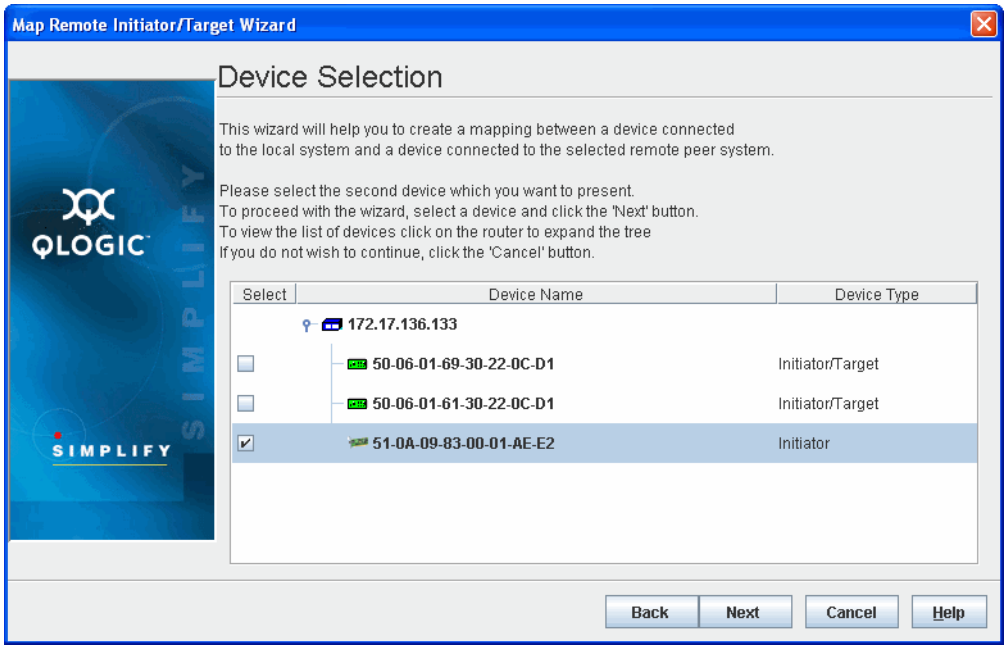

Map Remote Initiator/Target Wizard
Device Selection
This wizard will help you to create a mapping between a device connected
to the local system and a device connected to the selected remote peer system.
Please select the second device which you want to present.
To proceed with the wizard, select a device and click the 'Next' button.
To view the list of devices click on the router to expand the tree
If you do not wish to continue, click the 'Cancel' button.
Select
Device Name
Device Type
172.17.136.133
50-06-01-69-30-22-0C-D1
Initiator/Target
50-06-01-61-30-22-0C-D1
Initiator/Target
51-0A-09-83-00-01-AE-E2
Initiator
Back
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 7-73 Device Selection Dialog Box

3. If necessary, expand the router tree to see the attached devices. Select the device to be mapped. The device may be a target or an initiator and may be on either the remote router or on the local router. Click **Next.**

The port selection dialog box prompts you to select a port the system will use to connect to the device, as shown in Figure 7-74.

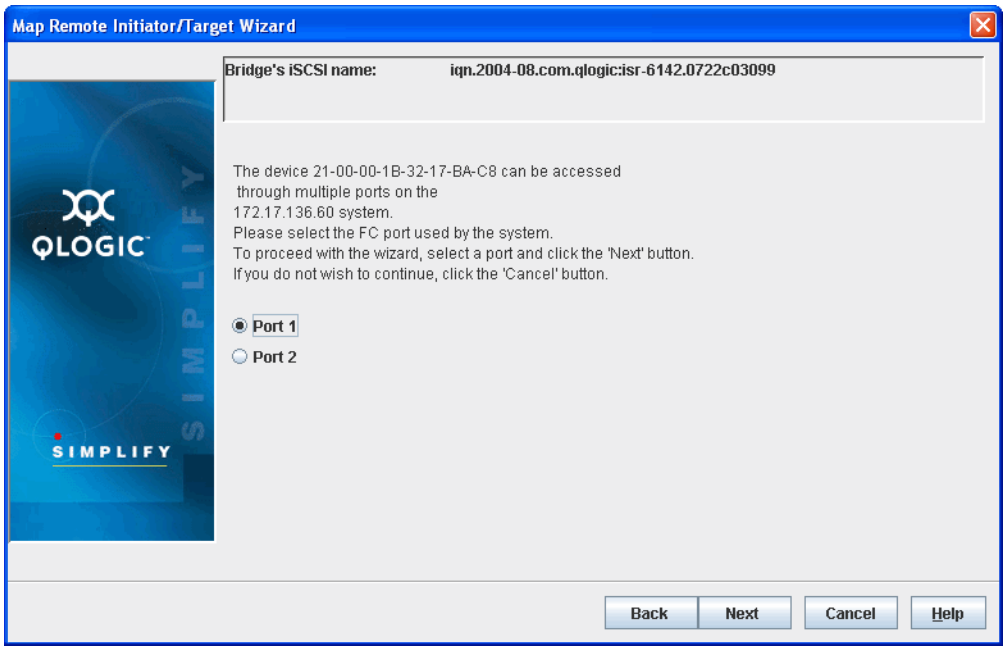


Figure 7-74 Port Selection Dialog Box

4. Select the port the system will use to connect to the device, then click **Next**.

The **Device Mapping Option** dialog box displays SmartWrite mapping options, as shown in Figure 7-75.

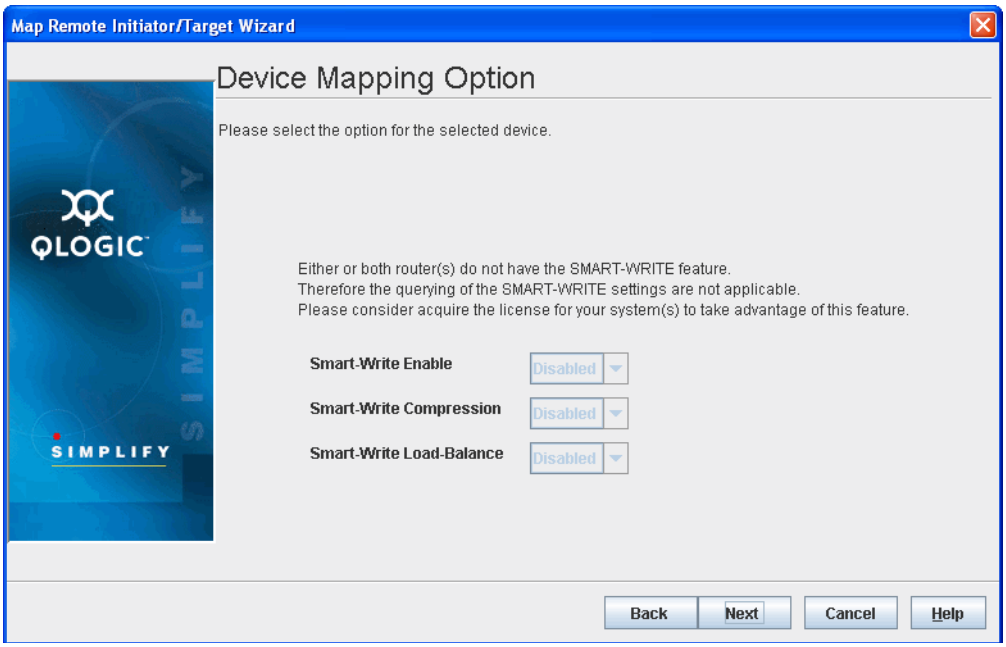


Figure 7-75 Device Mapping Option Dialog Box

5. If your router includes the SmartWrite feature, **Enable** or **Disable** the options as you want.
6. Click **Next.**

The **Confirm Mapping** dialog box displays the mapping and option selections, as shown in Figure 7-76.

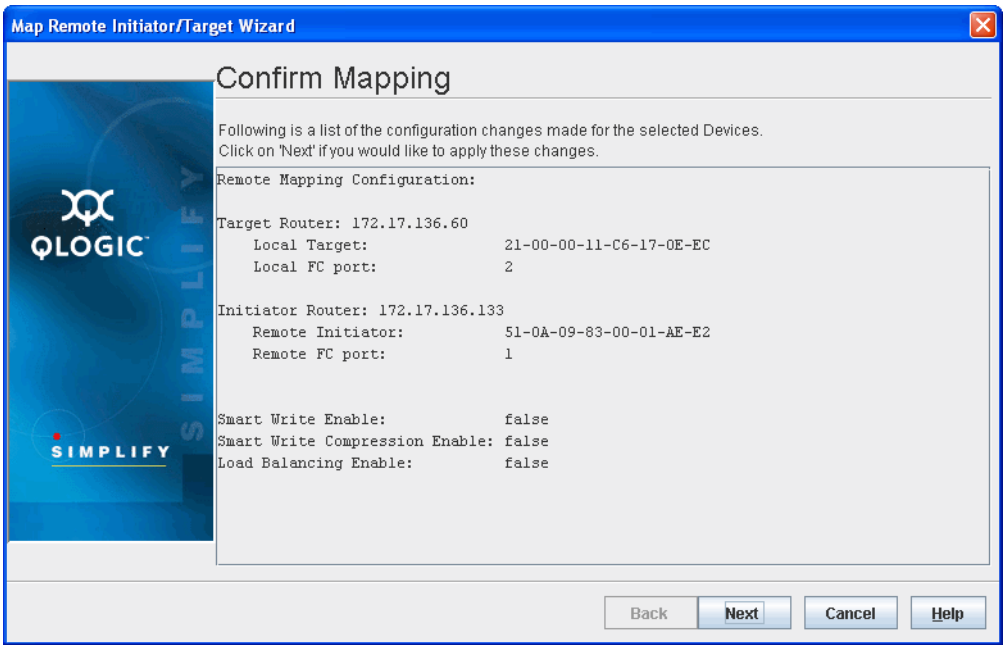


Figure 7-76 Confirm Mapping Dialog Box

7. Review the information and, if correct, click **Next**.

   The **Local Router Admin Password** dialog box displays, as shown in Figure 7-77.

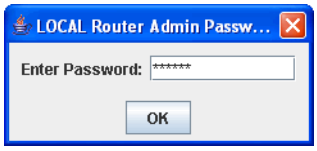


Figure 7-77 Local Password Dialog Box

8. Type the local router admin password (default=config), then click **OK**.

The Remote Mapping Status screen displays a list of newly mapped devices, as shown in Figure 7-78.

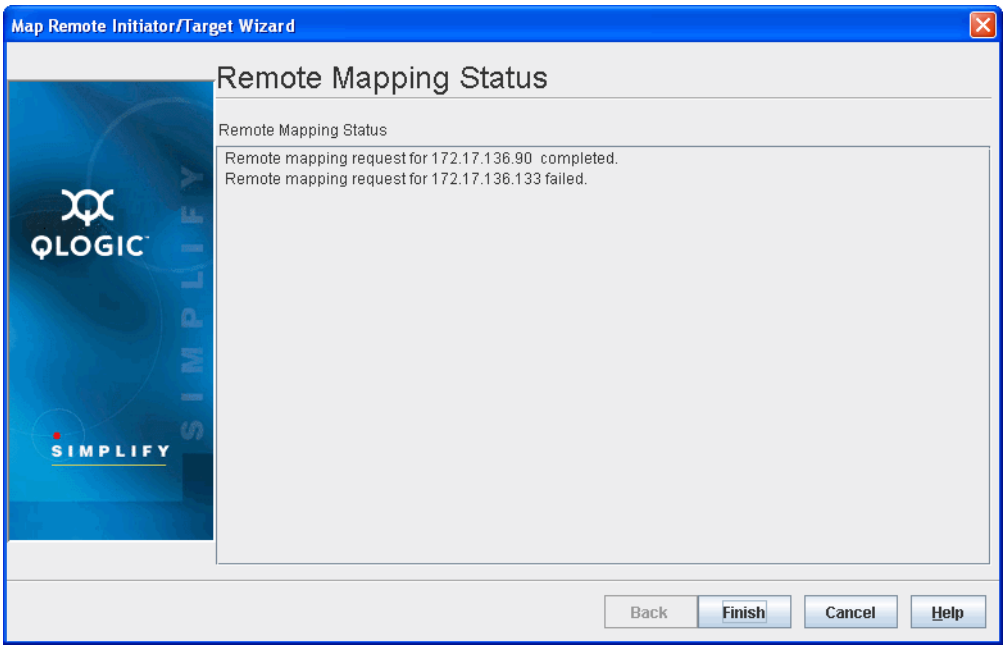


Figure 7-78 Local Router Admin Password Dialog Box

9. Review the status information, then click **Finish**.

   The system prompts you to refresh the display, as shown in Figure 7-79.

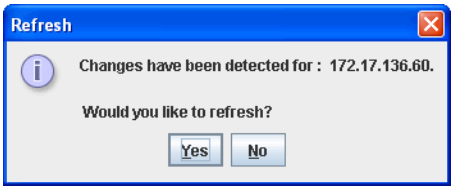


Figure 7-79 Refresh Screen

10. Click **Yes** to refresh the display.

11. View the mapped devices in the router's tree window. Figure 7-80 shows the mapping created in the sample procedures.

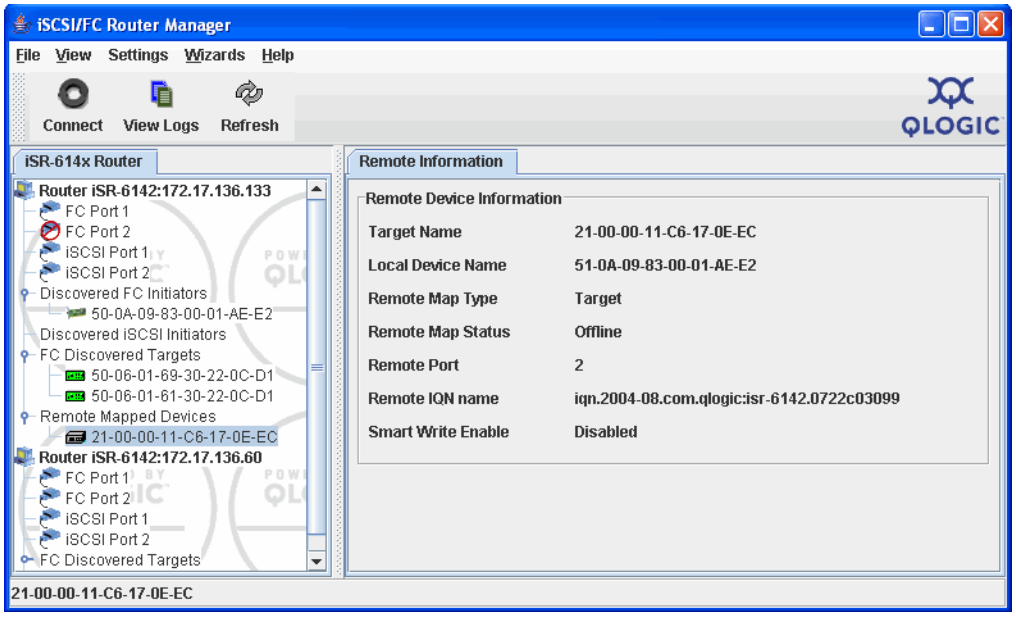


Figure 7-80 Remote Mapped Device

Unmap Remote Initiator/Target Wizard

The Unmap Remote Initiator/Target Wizard provides a set of dialog boxes that walk you through the steps required for removing an initiator-to-target mapping.

You can start this wizard at any time by selecting **Unmap Remote Initiator/Target Wizard** from the **Wizards Menu** or from the **Action Menu**.

When the Unmap Remote Initiator/Target wizard launches, the **Device Selection** dialog box displays a list of remote mapped devices, as shown in Figure 7-81.

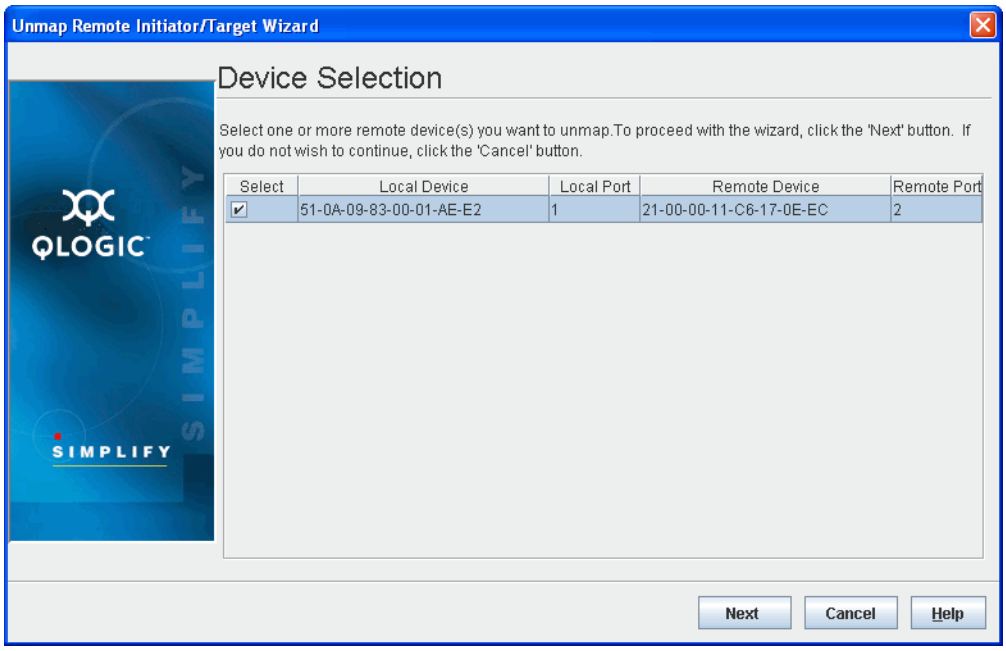


Figure 7-81 Device Selection Dialog Box

To unmap an initiator and target:

1. Select the device to be unmapped, then click **Next**.

The **Local Router's Admin Password** dialog box requests the local router's admin password to continue with the unmap, as shown in Figure 7-82.

Figure 7-82 Local Router Admin Password Dialog Box

2. Type the local router's admin password (default=config), then click **OK**.

   The **Remote Unmap Initiator-Target Status** dialog box displays the status of the unmap operation, as shown in Figure 7-83.

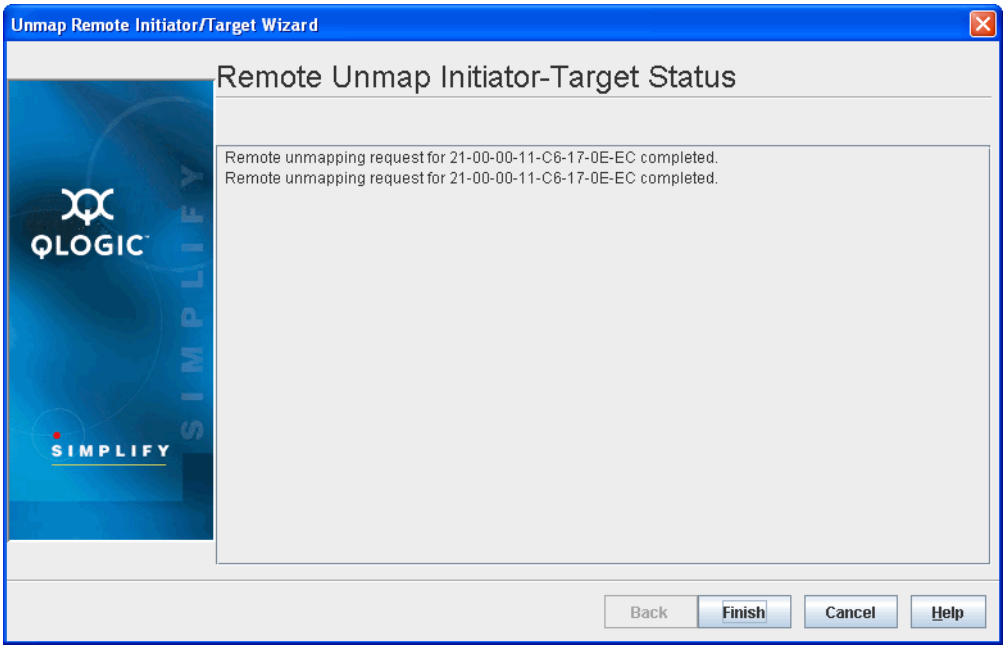


Figure 7-83 Remote Unmap Initiator-Target Status Dialog Box

3. Review the status, then click **Finish**.

Discover iSCSI Target Wizard

The Discover iSCSI Target Wizard provides a set of dialog boxes that walk you through the steps required for discovering an iSCSI target.

You can start this wizard at any time by selecting **Discover iSCSI Target** from the **Wizards Menu** or from the **Action Menu**.

When the Discover iSCSI Target wizard launches, the first window requests you to enter data: an IP address for the iSCSI target, the target's TCP port number (default is 3260) and the router's GE port to be used for the discovery, as shown in Figure 7-84.

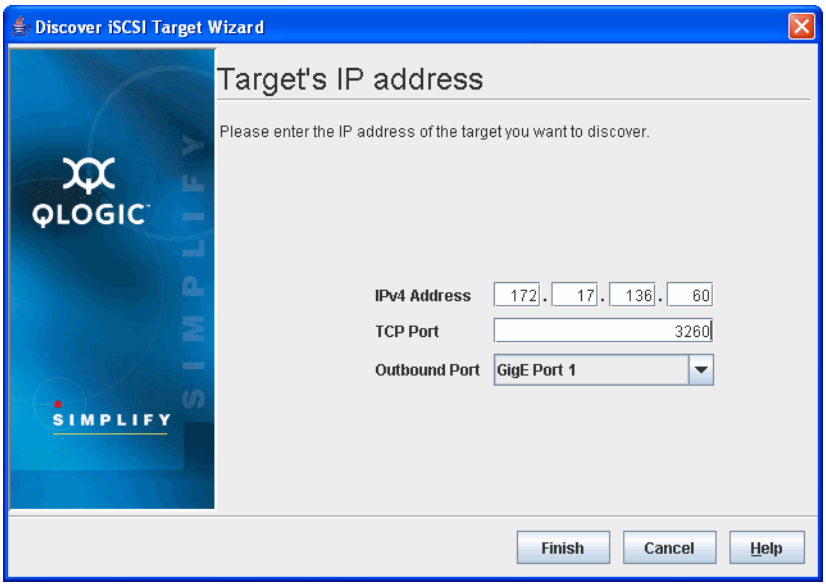


Figure 7-84 Discover iSCSI Target Wizard—IP Address Dialog Box

To discover an iSCSI target:

1. Enter the IP address.
2. Select the GE port from the **Outbound Port** drop-down list.
3. Click **Finish** to initiate the discovery operation.

   The **Security Check** dialog box requests the administrator password, as shown in Figure 7-85.

Figure 7-85 Discover iSCSI Target Wizard—Security Check Dialog Box

4. Type the appropriate password, then click **OK** to confirm the discovery of the iSCSI target.

   If the wizard detected iSCSI targets, the **Refresh** dialog box signifies the discovery of the iSCSI target, as shown in Figure 7-86. This dialog box may take a few seconds before appearing.

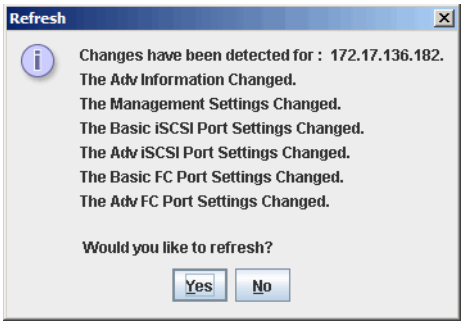

Refresh
Changes have been detected for : 172.17.136.182.
The Adv Information Changed.
The Management Settings Changed.
The Basic iSCSI Port Settings Changed.
The Adv iSCSI Port Settings Changed.
The Basic FC Port Settings Changed.
The Adv FC Port Settings Changed.
Would you like to refresh?
Yes
No

Figure 7-86 Discover iSCSI Target Wizard—Refresh Dialog Box

5. Click **Yes** to refresh system tree with the discovered iSCSI target, or click **No** to skip the refresh.

   After the refresh is complete, you can see the Discovered iSCSI Target in the system tree, as shown in Figure 7-87.

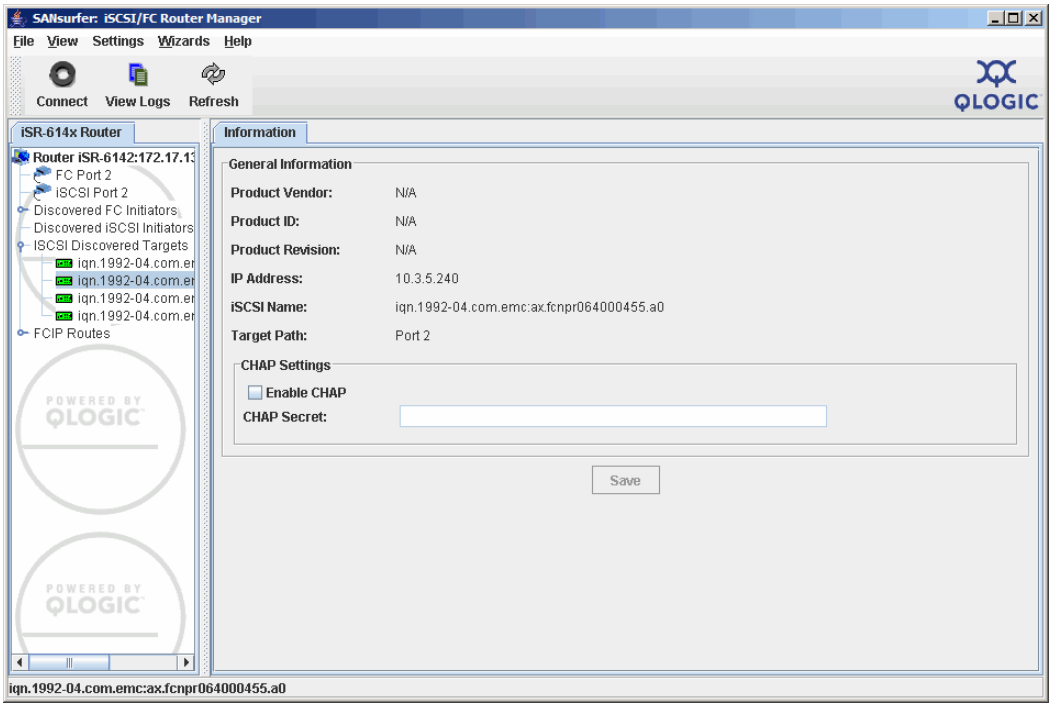


Figure 7-87 iSCSI Discovered Targets

FCIP Route Add Wizard

The FCIP Route Add Wizard provides a set of dialog boxes that walk you through the steps required for adding an FCIP route.

You can start this wizard at any time by selecting **FCIP Route Add** from the **Wizards Menu** or from the **Action Menu**.

When the FCIP Route Add Wizard launches, it displays a warning message, letting you know the operation may drop the connection to the selected GE and FC ports. If the router uses the selected ports in FC or iSCSI mappings, it will lose connectivity to them. Using this wizard will also momentarily disrupt connectivity on the GE port not selected for the FCIP route.

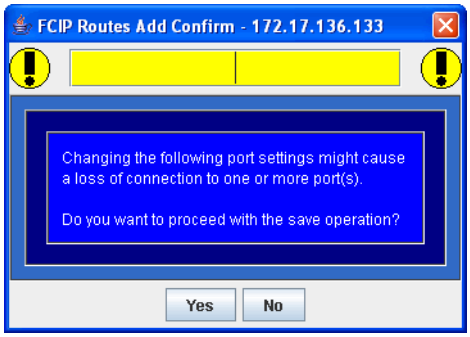

FCIP Routes Add Confirm - 172.17.136.133
Changing the following port settings might cause a loss of connection to one or more port(s).
Do you want to proceed with the save operation?
Yes
No

Figure 7-88 FCIP Route Add Wizard—Warning Dialog Box

To add an FCIP route:

1. Read the warning. If you want to proceed, click **Yes** and continue with step 2. Otherwise, click **No** to cancel the wizard.

The **FC and GigE Port Selection** dialog box prompts you to select an FC-GigE port pair, as shown in Figure 7-89.

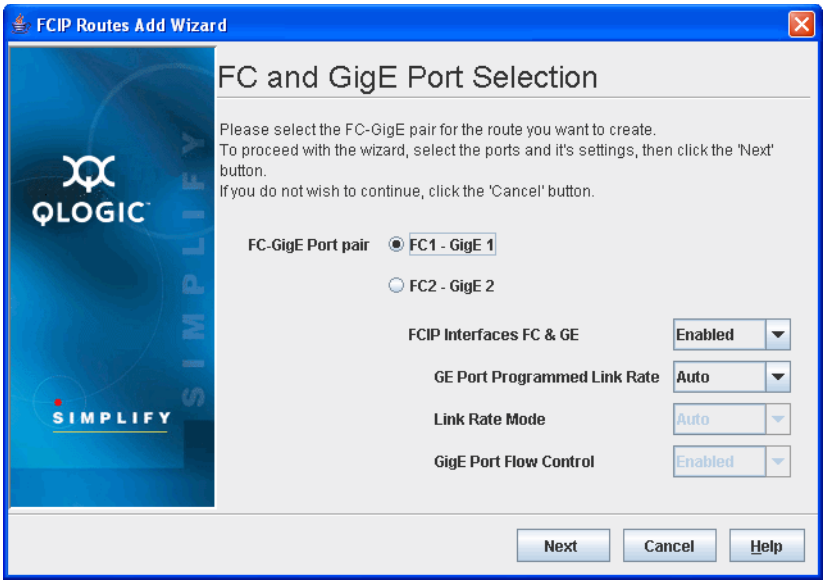

FCIP Routes Add Wizard
FC and GigE Port Selection
Please select the FC-GigE pair for the route you want to create.
To proceed with the wizard, select the ports and it's settings, then click the 'Next' button.
If you do not wish to continue, click the 'Cancel' button.
FC-GigE Port pair
FC1 - GigE 1
FC2 - GigE 2
FCIP Interfaces FC & GE
Enabled
GE Port Programmed Link Rate
Auto
Link Rate Mode
Auto
GigE Port Flow Control
Enabled
Next
Cancel
Help
QLOGIC
SIMPLIFY

Figure 7-89 FCIP Route Add Wizard—Port Selection Dialog Box

2. Select the FC-GigE Port pair. The corresponding parameter options become available.
3. If desired, configure the following port route/parameters:
   - **FCIP Interfaces FC & GE** – Provides a drop-down box you can use to enable or disable the FCIP route. Disabling the route places the FC and GE ports in a down state. It still retains all route configuration parameters.
   - **GigE Port Programmed Link Rate** – Provides a drop-down box you can use select one of four options for the GigE link rate: auto, 10, 100, or 1000. The default link rate is auto.
   - **Link Rate Mode** – Provides a drop-down box you can use select one of three options for the link rate mode: auto, half duplex, or full duplex. This dialog box is available only when the GigE link rate is set to something other than auto.
   - **GigE Port Flow Control** – Provides a drop-down box you can use to enable or disable GigE port flow control. The default is enabled. This dialog box is available only when the GigE link rate is set to something other than auto.
4. After selecting a port pair and setting GE port parameters, click **Next** to continue or click **Cancel** to quit the wizard.

The **Local and Remote IP Address** dialog box requests entry of IP addresses (see Figure 7-90).

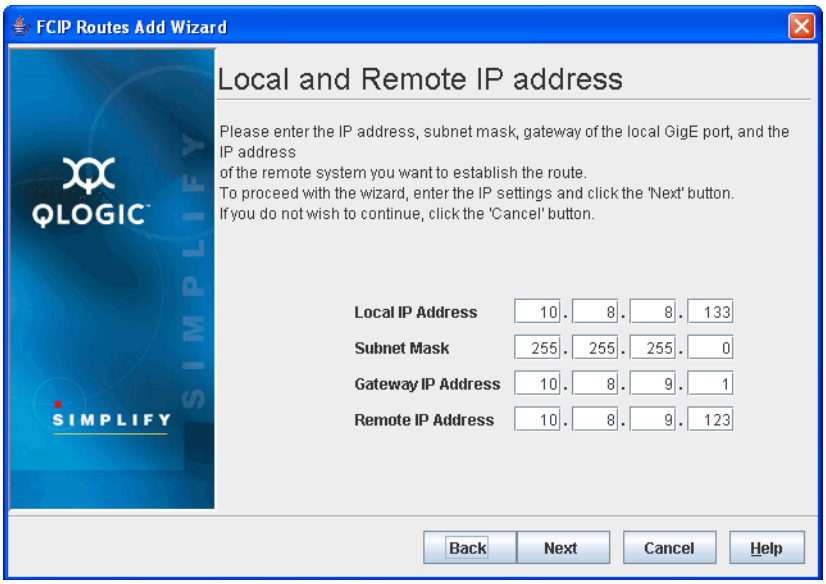

FCIP Routes Add Wizard
Local and Remote IP address
Please enter the IP address, subnet mask, gateway of the local GigE port, and the IP address
of the remote system you want to establish the route.
To proceed with the wizard, enter the IP settings and click the 'Next' button.
If you do not wish to continue, click the 'Cancel' button.
QLOGIC
SIMPLIFY
Local IP Address 10 . 8 . 8 . 133
Subnet Mask 255 . 255 . 255 . 0
Gateway IP Address 10 . 8 . 9 . 1
Remote IP Address 10 . 8 . 9 . 123
Back
Next
Cancel
Help

Figure 7-90 FCIP Route Add Wizard—Local and Remote IP Address Dialog Box

5. Configure any of the following parameters:
   - **Local IP Address** – Enter the IP address the GigE port will use. An uninitialized port has an IP address of all zeros.
   - **Subnet Mask** – Enter the subnet mask the GigE port will use.
   - **Gateway IP Address** – Enter the gateway IP address the GigE port will use.
   - **Remote IP Address** – Enter the IP address of the GigE port the GigE port will use on the remote router.
6. After setting the IP address parameters, click **Next** to continue or click **Cancel** to quit the wizard.

The **TCP/IP Options** dialog box requests entry of TCP/IP parameters, as shown in Figure 7-91.

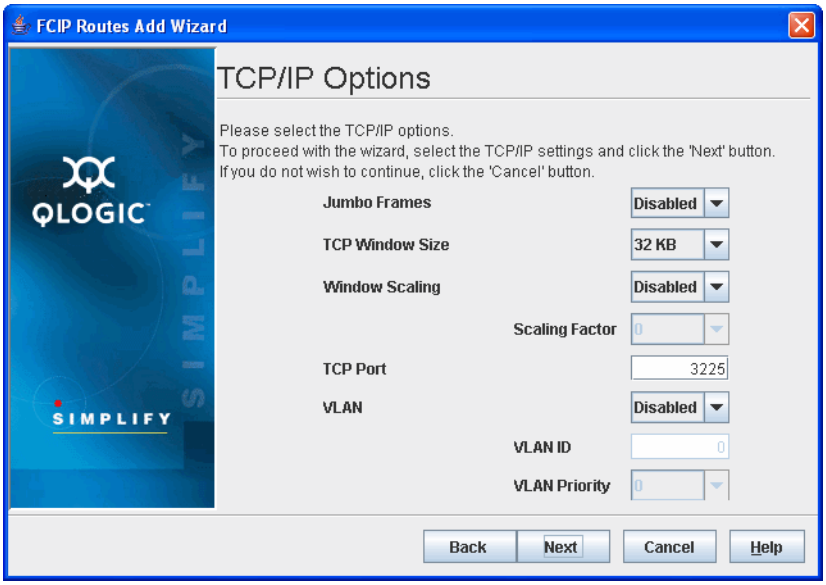


Figure 7-91 FCIP Route Add Wizard—TCP/IP Options Dialog Box

7. Configure any of the following parameters:

   - **Jumbo Frames** – Provides a drop-down box you can use to enable or disable Jumbo IP frames. When disabled the MTU is 1500 bytes. When enabled the MTU is 9000 bytes.
   - **TCP Window Size** – Provides a drop-down box you can use select one of three options for TCP window size: 8192, 16384, or 32768 bytes. The default is 32768.
   - **Window Scaling** – Provides a drop-down box you can use to enable or disable window scaling. The default is disabled.
   - **Window Scaling Factor** – Provides a drop-down box you can use select one of six options for TCP window scaling, any number between 0–5.
   - **VLAN Enabled** – Provides a drop-down box you can use to enable or disable VLAN support. The default is disabled.
   - **VLAN ID** – Provides a text field you can use to enter the VLAN ID. This option is available only when VLAN is enabled. The VLAN ID must be the same on both routers participating in the FCIP route (that is, local and remote routers must be using same VLAN ID) and the Ethernet switches.

- **VLAN Priority** – Provides a drop-down box that contains eight options for the VLAN priority: any number between 0–7. This dialog box is available only when VLAN is enabled.

8. After setting the TCP/IP parameters, click **Next** to continue or click **Cancel** to quit the wizard.

   The **FCIP Options** dialog box requests entry of FCIP parameters, as shown in Figure 7-92.

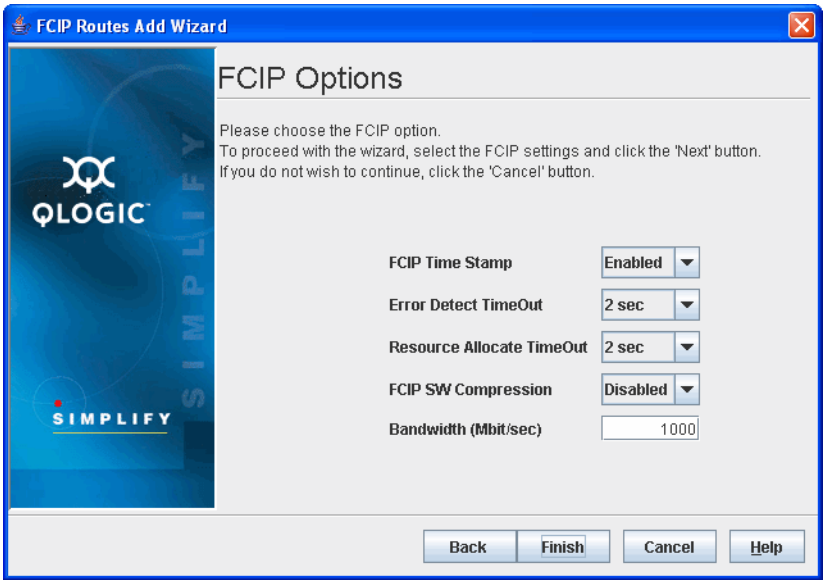


Figure 7-92 FCIP Route Add Wizard—FCIP Options Dialog Box

9. Configure any of the following parameters:

   - **FCIP Timestamp** – Provides a drop-down box you can use to enable or disable FCIP timestamps. The default is enabled.
   - **Error Detect Timeout** – Provides a drop-down box you can use to select one of five options for the error detect timeout: any number between 1 to 5 seconds. The default is one second.
   - **Resource Allocate Timeout** – Provides a drop-down box you can use to select one of five options for the resource allocate timeout: any number between 1 to 5 seconds. The default is one second.
   - **FCIP SW Compression** – Provides a drop-down box you can use to enable or disable FCIP compression. The default is disabled.
   - **Bandwidth (Mbit/sec)** – Provides a text field in which you can enter the maximum bandwidth (in megabits per second) used by the GigE port during transmits. The range of values supported is 1 to 1000 megabits per second. This setting allows you to limit the bandwidth

used by the FCIP route so as to not consume all the available link bandwidth. For example, if the slowest link in the WAN being used is a DS-3 link, the maximum available bandwidth is 45 megabits per second. To limit the FCIP route to 33% of the overall link bandwidth set the bandwidth to 15 megabits per second.

10. After setting the FCIP parameters, click **Next** to continue or click **Cancel** to quit the wizard.

    The **Security Check** dialog box requests the administrator password, as shown in Figure 7-93.

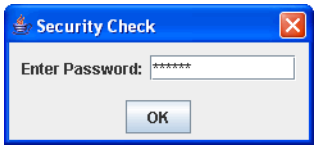


Figure 7-93 FCIP Route Add Wizard—Security Check Dialog Box

11. Type the appropriate password, then click **OK** to confirm adding the FCIP route.

    The **Add FCIP Route Complete** dialog box lets you know when the configuration is complete, as shown in Figure 7-94.

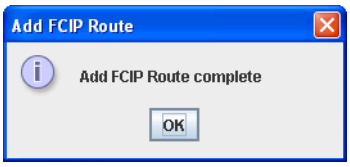


Figure 7-94 FCIP Route Add Wizard—Completed Dialog Box

NOTE:

This dialog box may take a few seconds before appearing.

12. Click **OK** to exit the dialog box.

FCIP Route Remove Wizard

The FCIP Route Remove Wizard provides a set of dialog boxes that walk you through the steps required for removing an FCIP route.

You can start this wizard at any time by selecting **FCIP Route Remove** from the **Wizards Menu** or from the **Action Menu**.

When the FCIP Route Remove wizard launches, it displays a warning message, letting you know the operation may drop the connection to the selected GE and FC ports. If the router uses the selected ports in FC or iSCSI mappings, it will lose connectivity to them. Using this wizard will also momentarily disrupt connectivity on the GE port not selected for the FCIP route.

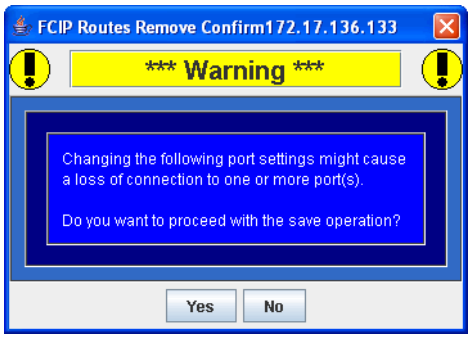

FCIP Routes Remove Confirm172.17.136.133
*** Warning ***
Changing the following port settings might cause a loss of connection to one or more port(s).
Do you want to proceed with the save operation?
Yes
No

Figure 7-95 FCIP Route Remove Wizard—Warning Dialog Box

To remove an FCIP route:

1. Read the warning. If you want to proceed, click **Yes** and continue with step 2. Otherwise, click **No** to cancel the wizard.

The FCIP Remove dialog box displays a list of existing FCIP routes, as shown in Figure 7-96.

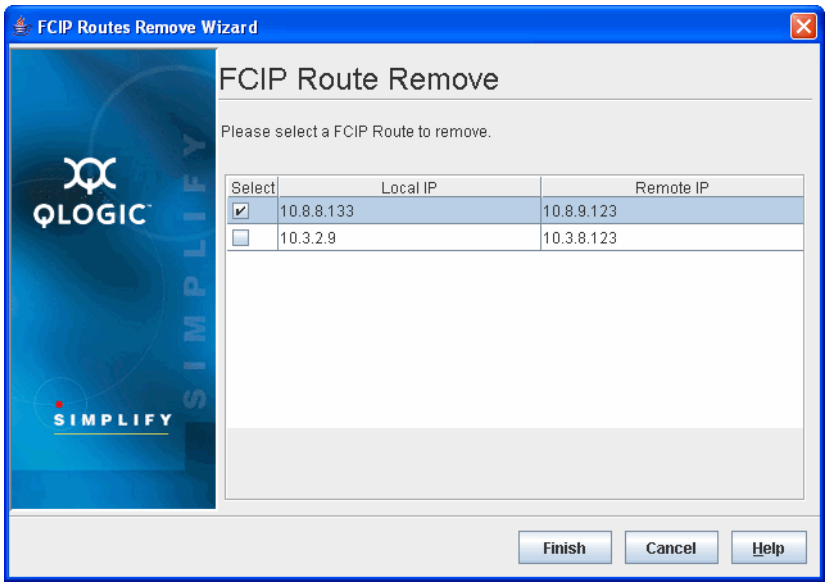


Figure 7-96 FCIP Route Remove Wizard—Route Selection Dialog Box

2. Select the FCIP route you want to remove, then click **Finish**.

   The **Security Check** dialog box requests the administrator password, as shown in Figure 7-97.

Figure 7-97 FCIP Route Remove Wizard—Security Check Dialog Box

3. Type the appropriate password, then click **OK** to confirm the removal of the FCIP route.

The **Add FCIP Route Complete** dialog box lets you know when the configuration is complete, as shown in Figure 7-98.

Figure 7-98 FCIP Route Remove Wizard—Completed Dialog Box

NOTE:

This dialog box may take a few seconds before appearing.

4. Click **OK** to exit the dialog box.

A Command Reference

The command line interface (CLI) enables you to perform a variety of router management tasks through an Ethernet or serial port connection. This section describes the following:

- Logging On to a SAN Router
- Guest Account
- Working with SAN Router Configurations
- Commands

Logging On to a SAN Router

To log on to a router using Telnet, open a command line window on the workstation and enter the Telnet command followed by the router IP address:

```
# telnet <ip_address>
```

A Telnet window opens prompting you for a login. Enter an account name and password.

To log on to a switch through the serial port, configure the workstation port with the following settings:

- 115200 baud
- 8-bit character
- 1 stop bit
- No parity

Enter an account name and password when prompted.

Guest Account

Routers come from the factory with the following account already defined:

Account name: guest

Password: password

This guest account provides access to the router and its configuration. After planning your router management needs, consider changing the password for this account.

The guest account is automatically closed after 15 minutes of inactivity.

See the Password Command for information about changing passwords.

Working with SAN Router Configurations

Successful management of routers with the command line interface depends on the effective use of router configurations. Modifying configurations, backing up configurations, and restoring configurations are key router management tasks.

Modifying a Configuration

The router has three major areas of configuration:

- Management port configuration, which uses the following commands:
  - Set Mgmt Command
  - Show Mgmt Command
- ISCSI port configuration, which uses the following commands:
  - Set iSCSI Command
  - Show iSCSI Command

Saving and Restoring Router Configurations

Saving and restoring a configuration can help protect your work or for use as a template in configuring other routers.

Save Router Configuration and Persistence

Perform the following steps to save the router's configuration and persistent data.

Persistent data consists of LUN mappings, discovered FC targets, and discovered iSCSI initiators.

1. Execute the Fru save CLI command (see FRU Command) to generate a file (`iSR-6142_FRU.bin`) containing the saved data. This file is stored locally on the router in an FTP directory.
2. Transfer the saved data from the router to a workstation by executing an FTP utility on a workstation. The following text is an example of an FTP transfer to get the saved router configuration data:

```
c:\>ftp 172.17.137.102
Connected to 172.17.137.102.
220 (none) FTP server (GNU inetutils 1.4.2) ready.
User (172.17.137.102:(none)): ftp
331 Guest login ok, type your name as password.
Password: ftp
230 Guest login ok, access restrictions apply.
ftp> bin
200 Type set to I.
ftp> get iSR-6142_FRU.bin
200 PORT command successful.
150 Opening BINARY mode data connection for
'iSR-6142_FRU.bin' (6168 bytes).
226 Transfer complete.
ftp: 6168 bytes received in 0.00Seconds
6168000.00Kbytes/sec.
ftp> quit
221 Goodbye.
```

Restore Router Configuration and Persistence

Perform the following steps to restore the router's configuration and persistent data:

1. Transfer the saved data from a workstation to the router by executing an FTP utility on the workstation. The following text is an example of an FTP transfer to put previously saved router configuration data on the router:

```
c:\>ftp 172.17.137.102
Connected to 172.17.137.102.
220 (none) FTP server (GNU inetutils 1.4.2) ready.
User (172.17.137.102:(none)): ftp
331 Guest login ok, type your name as password.
Password: ftp
230 Guest login ok, access restrictions apply.
ftp> bin
200 Type set to I.
ftp> put iSR-6142_FRU.bin
200 PORT command successful.
150 Opening BINARY mode data connection for
'iSR-6142_FRU.bin'.
226 Transfer complete.
ftp: 6168 bytes sent in 0.00Seconds
6168000.00Kbytes/sec.
ftp> quit
221 Goodbye.
```

2. Execute the Fru restore CLI command (see FRU Command) to update the router with the saved configuration data. The FRU restore command has the following two options:

   - Full restore – Restores all router configuration parameters, including IP addresses, subnet masks, gateways, Local/Remote mappings, and all other persistent data.
   - Partial restore – Restores only the Local/Remote mappings and persistent data, such as discovered FC targets and iSCSI initiators.

Commands

The CLI command syntax is as follows:

command

keyword

keyword *[value]*

keyword *[value1] [value2]*

The **command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case *insensitive*.
- Required keyword values appear in standard font: *[value]*. Optional values are shown in italics: *[value]*.
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example, the Delete keyword can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier.Table A-1 describes the command-line completion keystrokes.

Table A-1. Command Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press **Tab** key again to display all possibilities
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves cursor to the beginning of the command line.
Control-E	Moves cursor to the end of the command line.

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an Admin session. An account must have admin authority to enter the Admin Start command, which opens an admin session. Refer to the Admin Command.

Admin Command

Opens and closes an administrator session. You can run any command that changes the router configuration within an Admin session. Only one Admin session can be open on the router at any time. An inactive Admin session will time out after 15 minutes.

Authority None

Syntax **admin**

start (or begin)
end (or stop)
cancel

Keywords **start (or begin)**

Opens the Admin session.

end (or stop)

Closes the Admin session. The Logout, Shutdown, and Reset commands will also end an Admin session.

cancel

Terminates an Admin session opened by another user. Use this keyword with care, because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an Admin session does not release the session. In this case, you must either wait for the Admin session to time out, or use the Admin Cancel command.

Examples **Opening and closing an admin session example:**

```
QRouter #> admin start
Password : ******
QRouter(admin) #>
...
QRouter(admin) #> admin end
QRouter #>
```

Beacon Command

Enables or disables the Heartbeat and System Fault LEDs flashing. The heartbeat and system fault LEDs flash synchronously (on and off, together). No other LEDs are affected.

Authority Admin session

Syntax **beacon**

on

off

Keywords **on**

Turns on the router beacon.

off

Turns off the router beacon.

Examples **Beacon command example:**

```
QRouter #> beacon on
```

Clear Command

The clear command provides two operations: it removes all entries from the router's log file, or it resets the Fibre Channel and iSCSI statistic counters.

Authority Admin session

Syntax **clear [logs or stats]**

Keywords **logs**

Clears all entries from router's log file.

stats

Resets the statistic counters.

Examples **Clear command example:**

```
QRouter (admin) #> clear logs
QRouter (admin) #> clear stats
```

Date Command

This command displays or sets the date and time. To set the date and time, the information string must be provided in this format: *MMDDhhmmCCYY*. The new date and time takes effect immediately.

Authority Admin session to set the date and time. No authority required to display the current date and time.

Syntax **date**

[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***

Specifies the date—this requires an Admin session. If you omit *[MMDDhhmmCCYY],* the command uses the current date, which does not require an admin session.

Notes Network time protocol (NTP) must be disabled to set the time with the Date command. Refer to the Set NTP Command for information about NTP.

Examples **Date command example:**

```
QRouter (admin) #> date 010314282007
Tue Jan 1 14:28:00 2008
QRouter (admin) #> date
Tue Jan 1 14:28:14 2008
```

FcipRoute Command

The FCIP route command provides for configuring a new FCIP route and modifying or deleting an existing FCIP route. Each FCIP route requires a dedicated FC and Gigabit Ethernet port. Configuring an FCIP route, specifying an FC and GE port pair, take precedence over any previous configuration for the port pair (FC/GE). This removes the previous configuration of the port pair.

Authority Admin session.

Syntax **fciproute**
add
mod
rm

Keywords **add**

The FCIP route add command configures a new FCIP route.

modify

The FCIP route modify command modifies an existing FCIP route.

remove

The FCIP route remove command removes an existing FCIP route.

Examples **FCIP route add command example:**

```
QRouter (admin) #> fciproute add

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

WARNING:
The following command might cause a loss of connections to both GE
ports.

Configuring FCIP Route: 1
--------------------------
FCIP Interfaces FC & GE (0=Enable, 1=Disable) [Enabled         ]
FC Port (1=FC1, 2=FC2, ...)                   [FC1             ]
GE Port (1=GE1, 2=GE2, ...)                   [GE1             ]
IP Address (IPv4 or IPv6; 0=IPv6 Link Local)  [0.0.0.0         ] 0
Selected IPv6 Link Local Address: fe80::2c0:ddff:fe0c:8be2
```

```
Remote IPv6 Address                                [::              ]
fe80::21b:21ff:fe06:d517
MTU Size (0=Normal, 1=Jumbo, 2=Other)              [Normal          ]
TCP Window Size (0=8KB, 1=16KB, 2=32KB)            [32768           ]
Window Scaling (0=Enable, 1=Disable)               [Disabled        ]
TCP Port No. (Min=1024, Max=65535)                 [3225            ]
GE Port Speed (0=Auto, 1=100Mb, 2=1Gb)             [Auto            ]
FCIP Time Stamp (0=Enable, 1=Disable)              [Enabled         ]
Resource Allocate TimeOut (Min=1sec, Max=5sec)     [1               ]
Bandwidth, Mbit/sec (Min=1, Max=1000)              [1000            ]
VLAN (0=Enable, 1=Disable)                         [Disabled        ]
FCIP SW Compression (0=Enable, 1=Disable)          [Disabled        ]

  All attribute values for FCIP Route 1 will now be saved.
```

FCIP route modify command example:

```
QRouter (admin) #> fciproute mod

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

WARNING:
The following command might cause a loss of connections to both GE
ports.

  Route   FC Port ID  GE Port ID
  -----   ----------  ----------
  1       FC1         GE1

  Please select a FCIP route from the list above ('q' to quit): 1

  Configuring FCIP Route: 1
  --------------------------
  FCIP Interfaces FC & GE (0=Enable, 1=Disable) [Enabled         ]
  IP Address (IPv4 or IPv6; 0=IPv6 Link Local)  [::              ]
  Selected IPv6 Link Local Address: fe80::2c0:ddff:fe0c:8be2
  Remote IPv6 Address [fe80::21b:21ff:fe06:d517]
fe80::21b:21ff:fe06:d514
  MTU Size (0=Normal, 1=Jumbo, 2=Other)         [Normal          ]
```

```
TCP Window Size (0=8KB, 1=16KB, 2=32KB)        [32768          ]
Window Scaling (0=Enable, 1=Disable)           [Disabled       ]
TCP Port No. (Min=1024, Max=65535)             [3225           ]
GE Port Speed (0=Auto, 1=100Mb, 2=1Gb)         [Auto           ]
FCIP Time Stamp (0=Enable, 1=Disable)          [Enabled        ]
Resource Allocate TimeOut (Min=1sec, Max=5sec)[1              ]
Bandwidth, Mbit/sec (Min=1, Max=1000)          [1000           ]
VLAN (0=Enable, 1=Disable)                     [Disabled       ]
FCIP SW Compression (0=Enable, 1=Disable)      [Disabled       ]

All attribute values for FCIP Route 1 will now be saved.
```

FCIP route remove command example:

```
QRouter (admin) #> fciproute rm

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

WARNING:
The following command might cause a loss of connections to both GE
ports.

Route   FC Port ID  GE Port ID
-----   ----------  ----------
1       FC1         GE1

Please select a FCIP route from the list above ('q' to quit): 1

FCIP Route 1 has been removed from the system.
```

FRU Command

The FRU command saves and restores the router's configuration.

Authority Admin session to restore.

Syntax **fru**

restore
save

Keywords **restore**

The FRU restore command requires that you first ftp the tar file containing the desired configuration to the router. After issuing this command, you are prompted for the restore level. You can fully restore the router's configuration (all configuration parameters and LUN mappings) or restore only the LUN mappings. The restored configuration will not take effect until you reboot the router.

save

The FRU save command creates a tar file containing the router's persistent data, configuration, and LUN mappings. It stores the file in the router's /var/ftp directory. You must then ftp the tar file from the router.

Examples **FRU restore command example:**

```
QRouter (admin) #> fru restore
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Type of restore (0=full, 1=mappings only) [full]

FRU restore completed.
Please reboot the system for configuration to take effect.
```

FRU save command example:

```
QRouter (admin) #> fru save

FRU save completed. Configuration File is QLogic_Router_FRU.bin
Please use FTP to extract the file out from the System.
```

Help Command

The help command displays a list of the commands and their syntax.

Authority None

Syntax **help**

Examples **Help command example:**

```
QRouter #> help
amin [ cancel | start | end ]
beacon [ on | off ]
date [ <MMDDhhmmCCYY> ]
clear [ logs | stats ]
fciproute [ add | mod | rm ]
discover
fru [ restore | save ]
history
image [ cleanup | list | unpack ]
image cleanup
image list
image unpack [ <filename> ]
initiator [ add | rm ]
localmap [ add | rm ]
logout
passwd
ping
quit
reboot
remotemap [ add | mod | rm ]
remotepeer [ add | rm ]
reset factory
save [ capture | logs | traces ]
set [ chap | fc | features | iscsi
isns | mgmt | ntp | properties
snmp | system ]
set chap
set fc [ <PORT_NUM> ]
set features
set iscsi [ <PORT_NUM> ]
set isns [ <PORT_NUM> ]
set mgmt
set ntp
set properties
set snmp [trap_destinations [ <DEST_NUM> ]]
set system
show [ chap | fc | fciproutes
features | initiators | iscsi
isns | localmaps | logs
```

```
memory | mgmt | ntp
perf | presented_initiators | presented_targets
properties | remotemaps | remotepeers
snmp | stats | system
targets ]
show chap
show fc [ <PORT_NUM> ]
show fciproutes [ <LINK_ID> ]
show features
show initiators [ fc | iscsi ]
show iscsi [ <PORT_NUM> ]
show isns [ <PORT_NUM> ]
show localmaps
show logs
show memory
show mgmt
show ntp
show perf [ byte | init_rbyte | init_wbyte | tgt_rbyte | tgt_wbyte ]
show presented_initiators [ fc | iscsi ]
show presented_targets [ fc | iscsi ]
show properties
show remotemaps
show remotepeers
show snmp
show stats
show system
show targets [ fc | iscsi ]
shutdown
target [ add | rm ]
```

History

Displays a numbered list of the previously entered commands.

Authority None

Syntax **History**

Examples **History command example:**

```
QRouter (admin) #> history
1: admin start
2: help
3: history
```

Image Command

Updates the router's firmware image and cleans up (removes) the image files in the router's /var/ftp directory.

NOTE:

Use FTP to transfer an image file to the router's /var/ftp directory.

Authority Admin session

Syntax **image**

cleanup
list
unpack [file]

Keywords **cleanup**

Removes all firmware image files in the router's /var/ftp directory. You can transfer these are files when updating the router's firmware image.

list [file]

Displays a list of the firmware image files in the router's /var/ftp directory.

unpack [file]

Unpacks the firmware image file specified in the [file] parameter and installs the firmware image on the router. You must reboot the router to activate the new firmware image.

Image cleanup command example:

```
QRouter (admin) #> image cleanup
```

Image list command example:

```
QRouter (admin) #> image list
isr-6142-2_1_1_0.bin
```

Image unpack command example:

```
QRouter (admin) #> image unpack isr-6142-2_1_1_0.bin
Unpack Completed. A reboot is required for the FW to take effect.
Do you wish to reboot the System at the current time (y/n): n
```

Initiator Command

Adds, modifies, and removes an initiator in the router's database.

Authority Admin session

Syntax **initiator**
add
mod
remove

Keywords **add**

Adds an initiator the router's database.

mod

Modifies the settings of an initiator.

remove

Removes an initiator.

Examples **Initiator add command example:**

```
QRouter (admin) #> initiator add

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

iSCSI Initiator Name (Max = 256 characters) [ ]
iqn.1991-05.com.microsoft:qlogic-09sd5i4l
All attribute values for that have been changed will now be saved.
```

Initiator mod (modify) command example:

```
QRouter (admin) #> initiator mod
Index (WWNN/iSCSI Name)
----- -----------------
0 iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Please select an Initiator from the list above ('q' to quit): 0

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

All attribute values for that have been changed will now be saved.
```

Initiator remove command example:

```
QRouter (admin) #> initiator rm
Index (WWNN/iSCSI Name)
----- -----------------
0 iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Please select an Initiator from the list above ('q' to quit): 0 All
attribute values for that have been changed will now be saved.
```

Localmap Command

The localmap command maps a locally-connected initiator device to a locally-connected target device. The initiator and target are not on the same FC port.

Authority Admin session

Syntax **localmap**

add

rm

Keywords **add**

Add local initiator to target mapping.

rm

Remove local initiator to target mapping.

Examples **Localmap add command example with FC port query:**

```
QRouter (admin) #> localmap add

The following wizard will query for attributes before persisting and
activating the updated mapping in the system configuration. If you
wish to terminate this wizard before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 50:06:01:60:b0:22:0c:d1,50:06:01:68:30:22:0c:d1
1 iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Please select an Initiator from the list above ('q' to quit) : 1

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:20:37:fd:9c:f7,22:00:00:20:37:fd:9c:f7
1 50:06:01:60:b0:22:0c:d1,50:06:01:68:30:22:0c:d1
2 20:00:00:20:37:fd:8a:b0,22:00:00:20:37:fd:8a:b0
3 20:00:00:20:37:fd:8b:ab,22:00:00:20:37:fd:8b:ab

Please select a Target from the list above ('q' to quit) : 3
iSCSI port used to access the Initiator (1=GE1, 2=GE2, ...) : 2
FC port used to access the Target (1=FC1, 2=FC2, ...) : 1

The selected initiator has not been presented on the port that was
selected to access the target. The following steps in the wizard will
now setup the initiator so that it is presented on the port that will
be used to access the target. A default name for the presented
```

```
initiator is assigned below. To accept the default assigned name
simply press the ENTER key or enter a new name.

FC presented initiator WWPN [21:01:00:c0:dd:0c:8b:e2 ] :

The selected target has not been presented on the port that was
selected to be accessed the initiator. The following steps in the
wizard will now setup the target so that it is presented on the port
that will be used by the initiator. A default name for the presented
target is assigned below. To accept the default assigned name simply
press the ENTER key or enter a new name.

iSCSI presented target name
[iqn.2004-08.com.qlogic:isr-6142.0608a00471.1.220000
2037fd8bab.2000002037fd8bab] :

All attribute values for that have been changed will now be saved.
```

Localmap add command example without FC port query:

```
QRouter (admin) #> localmap add

The following wizard will query for attributes before persisting and
activating the updated mapping in the system configuration. If you
wish to terminate this wizard before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 50:06:01:60:b0:22:0c:d1,50:06:01:68:30:22:0c:d1
1 iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Please select an Initiator from the list above ('q' to quit) : 1

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:20:37:fd:9c:f7,22:00:00:20:37:fd:9c:f7
1 50:06:01:60:b0:22:0c:d1,50:06:01:68:30:22:0c:d1
2 20:00:00:20:37:fd:8a:b0,22:00:00:20:37:fd:8a:b0
3 20:00:00:20:37:fd:8b:ab,22:00:00:20:37:fd:8b:ab

Please select a Target from the list above ('q' to quit) : 3
iSCSI port used to access the Initiator (1=GE1, 2=GE2, ...) : 2

The selected initiator has not been presented on the port that was
selected to access the target. The following steps in the wizard will
now setup the initiator so that it is presented on the port that will
be used to access the target. A default name for the presented
initiator is assigned below. To accept the default assigned name
simply press the ENTER key or enter a new name.
```

```
FC presented initiator WWPN [21:01:00:c0:dd:0c:8b:e2 ] :

The selected target has not been presented on the port that was
selected to be accessed the initiator. The following steps in the
wizard will now setup the target so that it is presented on the port
that will be used by the initiator. A default name for the presented
target is assigned below. To accept the default assigned name simply
press the ENTER key or enter a new name.
iSCSI presented target name
[iqn.2004-08.com.qlogic:isr-6142.0608a00471.1.220000
2037fd8bab.2000002037fd8bab] :

All attribute values for that have been changed will now be saved.
```

Localmap remove command example:

```
172.17.137.171 (admin) #> localmap rm

The following wizard will query for attributes before persisting and
activating the updated mapping in the system configuration. If you
wish to terminate this wizard before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:14:c3:44:9a:fa,22:00:00:14:c3:44:9a:fa
1 20:00:00:20:37:fd:9c:f7,22:00:00:20:37:fd:9c:f7
2 20:00:00:20:37:fd:8a:b0,22:00:00:20:37:fd:8a:b0
3 20:00:00:14:c3:44:9b:9d,22:00:00:14:c3:44:9b:9d
4 20:00:00:14:c3:3d:d2:bf,22:00:00:14:c3:3d:d2:bf
5 20:00:00:14:c3:44:9b:86,22:00:00:14:c3:44:9b:86
6 20:00:00:14:c3:3d:cf:80,22:00:00:14:c3:3d:cf:80
7 20:00:00:14:c3:44:9a:f1,22:00:00:14:c3:44:9a:f1
8 20:00:00:14:c3:44:9b:0b,22:00:00:14:c3:44:9b:0b
9 20:00:00:14:c3:44:9b:7c,22:00:00:14:c3:44:9b:7c

Please select a Target from the list above ('q' to quit): 0 The
following is a list of the initiators that have been mapped to the
selected target and the port that was configured for the initiator to
be presented on in order to access the target.

Target
Index Port Initiator (WWNN,WWPN/iSCSI Name)
----- ------ -------------------------------
0 FC1 iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Please select an Initiator to remove ('q' to quit) : 0

All attribute values for that have been changed will now be saved.
```

Logout Command

Exits the command line interface and returns you to the login prompt.

Authority None

Keywords **logout**

Examples **Logout command example:**

```
QRouter (admin) #> logout
(none) login:
```

Password Command

Changes the guest and administrator passwords.

Authority Admin session

Syntax **password**

Examples **Password command example:**

```
QRouter (admin) #> passwd
Press 'q' and the ENTER key to abort this command.
Select password to change (0=guest, 1=admin) : 1
account OLD password : ******
account NEW password (6-128 chars) : ******
please confirm account NEW password : ******
Password has been changed.
```

Ping Command

The ping command verifies the connectivity of each Ethernet port, management, GE1 (iSCSI 1), and GE2 (iSCSI 2).

Authority Admin session

Syntax **ping**

Examples **Ping command example:**

```
QRouter (admin) #> ping

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

IP Address (IPv4 or IPv6)                [0.0.0.0]
fe80::217:a4ff:fe99:c279
Iteration Count (0=Continuously)         [0      ] 10
Outbound Port (0=Mgmt, 1=GE1, 2=GE2, ...) [Mgmt   ]
Size Of Packet (Min=1, Max=65486 Bytes)  [56     ]

Pinging fe80::217:a4ff:fe99:c279 with 56 bytes of data:

Request timed out.
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.4ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.3ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.3ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.2ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.3ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.3ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.7ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.2ms
Reply from fe80::217:a4ff:fe99:c279: bytes=64 time=0.2ms

Ping Statistics for fe80::217:a4ff:fe99:c279:
Packets:  Sent  = 10,  Received = 9, Lost = 1
Approximate round trip times in milli-seconds:
Minimum = 0.2ms, Maximum = 0.7ms, Average = 0.3ms
```

Quit Command

Exits the command line interface and returns you to the login prompt.

Authority None

Syntax **quit**

Examples **Quit command example:**

```
QRouter (admin) #> quit
(none) login:
```

Reboot Command

Restarts the router firmware.

Authority Admin session

Syntax **reboot**

Examples **Reboot command example:**

```
QRouter (admin) #> reboot
Are you sure you want to reboot the System (y/n): y
System will now be rebooted...
```

Remote Map Command

The remotemap command provides for the mapping of an initiator and target, one of which is located on a remote system (router). It prompts you to enter the remote system (router), then lists the devices (initiators and targets) located on the remote system. You can select a device from the remote system and then the local system.

Authority Admin session

Syntax **remotemap**

add
mod
rm

Keywords **add**

Adds a device mapping, initiator to target, one of which is remote.

mod

Modifies an existing remote device mapping.

rm

Removes a remote device mapping.

Examples **Remotemap add command example:**

```
QRouter (admin) #> remotemap add

The following wizard will create a mapping a device connected to the
local system and a device connected to the selected remote peer
system. If you wish to terminate this wizard before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Index (System Info, Mgmt IP Address)
----- -----------------------------
0 iSR-6142.0608A00487(172.17.137.215)

Please select a REMOTE system from the list above ('q' to quit) : 0

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:20:00:d0:b2:02:86:d0,21:20:00:d0:b2:02:86:d0 (Init/Tgt)
1 20:21:00:d0:b2:02:86:d0,21:21:00:d0:b2:02:86:d0 (Init/Tgt)
2 20:20:00:d0:b2:02:86:d1,21:20:00:d0:b2:02:86:d1 (Init/Tgt)
3 20:21:00:d0:b2:02:86:d1,21:21:00:d0:b2:02:86:d1 (Init/Tgt)

Please select a LOCAL device from the list above ('q' to quit) : 0
```

```
Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:e0:8b:08:5f:3d,21:00:00:e0:8b:08:5f:3d (Initiator)
1 20:00:00:d0:b2:00:19:f0,21:00:00:d0:b2:00:19:f0 (Init/Tgt)

Please select a REMOTE device from the list above ('q' to quit) : 0

NOTE: Both the LOCAL and REMOTE systems do not have the SMART-WRITE
feature, therefore the querying of the SMART-WRITE settings are not
applicable and will be skipped for this mapping. All attribute values
for that have been changed will now be saved.
```

Remotemap add command example with SMART-WRITE licenses:

```
QRouter (admin) #> remotemap add

The following wizard will create a mapping a device connected to the
local system and a device connected to the selected remote peer
system. If you wish to terminate this wizard before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Index (System Info, Mgmt IP Address)
----- ------------------------------
0 iSR-6142.0608A00471(172.17.137.143)

Please select a REMOTE system from the list above ('q' to quit) : 0

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:01:00:e0:8b:28:5f:3d,21:01:00:e0:8b:28:5f:3d (Initiator)
1 20:00:00:e0:8b:08:5f:3d,21:00:00:e0:8b:08:5f:3d (Initiator)

Please select a LOCAL device from the list above ('q' to quit) : 0

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:14:c3:3d:d2:bf,22:00:00:14:c3:3d:d2:bf (Target)
1 20:00:00:14:c3:44:9b:86,22:00:00:14:c3:44:9b:86 (Target)
2 20:00:00:14:c3:44:9b:9d,22:00:00:14:c3:44:9b:9d (Target)
3 20:00:00:14:c3:44:9a:fa,22:00:00:14:c3:44:9a:fa (Target)
4 20:00:00:20:37:fd:9c:f7,22:00:00:20:37:fd:9c:f7 (Target)
5 20:00:00:20:37:fd:8a:b0,22:00:00:20:37:fd:8a:b0 (Target)
6 20:00:00:14:c3:3d:cf:80,22:00:00:14:c3:3d:cf:80 (Target)
7 20:00:00:14:c3:44:9a:f1,22:00:00:14:c3:44:9a:f1 (Target)
8 20:00:00:14:c3:44:9b:0b,22:00:00:14:c3:44:9b:0b (Target)
9 20:00:00:14:c3:44:9b:7c,22:00:00:14:c3:44:9b:7c (Target)
10 20:00:00:20:37:fd:8b:ab,22:00:00:20:37:fd:8b:ab (Target)

Please select a REMOTE device from the list above ('q' to quit) : 0
```

```
Smart-Write (0=Enable, 1=Disable) [Enabled ]
Smart-Write Compression (0=Enable, 1=Disable) [Disabled ]
Smart-Write Load Balance (0=Enable, 1=Disable) [Disabled ]
All attribute values for that have been changed will now be saved.
```

Remotemap add command example wihout SMART-WRITE licenses:

```
QRouter (admin) #> remotemap add

The following wizard will create a mapping a device connected to the
local system and a device connected to the selected remote peer
system. If you wish to terminate this wizard before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Index (System Info, Mgmt IP Address)
----- ------------------------------
0 iSR-6142.0608A00487(172.17.137.215)
Please select a REMOTE system from the list above ('q' to quit) : 0
Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:20:00:d0:b2:02:86:d0,21:20:00:d0:b2:02:86:d0 (Init/Tgt)
1 20:21:00:d0:b2:02:86:d0,21:21:00:d0:b2:02:86:d0 (Init/Tgt)
2 20:20:00:d0:b2:02:86:d1,21:20:00:d0:b2:02:86:d1 (Init/Tgt)
3 20:21:00:d0:b2:02:86:d1,21:21:00:d0:b2:02:86:d1 (Init/Tgt)

Please select a LOCAL device from the list above ('q' to quit) : 0

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:e0:8b:08:5f:3d,21:00:00:e0:8b:08:5f:3d (Initiator)
1 20:00:00:d0:b2:00:19:f0,21:00:00:d0:b2:00:19:f0 (Init/Tgt)
Please select a REMOTE device from the list above ('q' to quit) : 0

NOTE: Both the LOCAL and REMOTE systems do not have the SMART-WRITE
feature, therefore the querying of the SMART-WRITE settings are not
applicable and will be skipped for this mapping. All attribute values
for that have been changed will now be saved.
```

Remotemap modify command example with SMART-WRITE licenses:

```
QRouter (admin) #> remotemap mod

The following wizard will be used to modify various settings of a
remote mapping. If you wish to terminate this wizard before reaching
the end of the list press 'q' or 'Q' and the ENTER key to do so.

Index Local Device (WWPN) Remote Device (WWPN)
----- ------------------- --------------------
0 21:00:00:e0:8b:08:5f:3d 22:00:00:20:37:fd:8a:b0
```

```
Please select a remote mapping from the list above ('q' to quit): 0

Smart-Write Compression (0=Enable, 1=Disable) [Disabled ] 1
Smart-Write Load Balance (0=Enable, 1=Disable) [Enabled ] 1
All attribute values for that have been changed will now be saved.
```

Remotemap modify command example without SMART-WRITE licenses:

```
QRouter (admin) #> remotemap mod

The following wizard will be used to modify various settings of a
remote mapping. If you wish to terminate this wizard before reaching
the end of the list press 'q' or 'Q' and the ENTER key to do so.

Index Local Device (WWPN) Remote Device (WWPN)
----- ------------------- --------------------
0 21:20:00:d0:b2:02:86:d0 21:00:00:d0:b2:00:19:f0
1 21:21:00:d0:b2:02:86:d0 21:00:00:d0:b2:00:19:f0
2 21:20:00:d0:b2:02:86:d1 21:00:00:d0:b2:00:19:f0
3 21:21:00:d0:b2:02:86:d1 21:00:00:d0:b2:00:19:f0
4 21:20:00:d0:b2:02:86:d0 21:00:00:e0:8b:08:5f:3d

Please select a remote mapping from the list above ('q' to quit): 0

The SMART-WRITE feature license in not applicable for the selected
mapping. Only mappings with the SMART-WRITE feature can be modified by
this command.
Command aborted.
```

Remotemap remove command example:

```
QRouter (admin) #> remotemap rm

The following wizard will query for attributes before persisting and
activating the updated mapping in the system configuration. If you
wish to terminate this wizard before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Index Local Device (WWPN) Remote Device (WWPN)
----- ------------------- --------------------
0 21:00:00:e0:8b:08:5f:3d 22:00:00:14:c3:44:9a:fa
Please select a remote mapping from the list above ('q' to quit): 0
All attribute values for that have been changed will now be saved.
```

Remote Peer Command

The remotepeer command lets you assign a router peer to a local router, which can have up to four peers.

Authority Admin session

Syntax **remotepeer**

add
rm

Keywords **add**

Add a peer router.

rm

Remove a peer router.

Examples **Remotepeer add command example:**

```
QRouter (admin) #> remotepeer add

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

REMOTE MGMT port IP Address [0.0.0.0] 172.17.137.143
Contacting REMOTE system (timeout=120 seconds) ...
<Admin> password of REMOTE system: ******
<Admin> password confirmed.
Remote System Information
-------------------------
Product Name iSR-6142
Symbolic Name
Serial Number 0608A00471
HW Version 3
SW Version 2.3.0.1
No. of iSCSI Ports 2
iSCSI Base Name iqn.2004-08.com.qlogic:isr-6142.0608a00471
Mgmt IP Address 172.17.137.143
iSCSI Port 1 IP Address 10.3.5.106
iSCSI Port 1 TCP Port No. 3260
iSCSI Port 2 IP Address 10.3.5.107
iSCSI Port 2 TCP Port No. 3260
Do you wish to create a connection with the REMOTE system (y/n): y
All attribute values for that have been changed will now be saved.
```

Remotepeer remove command example:

```
QRouter (admin) #> remotepeer rm

Index (System Info, Mgmt IP Address)
----- ------------------------------
0 iSR-6142.0608A00487(172.17.137.215)

Please select a remote system from the list above ('q' to quit): 0

WARNING:
Remote mappings exist between the LOCAL system and the selected REMOTE
system. Removing this REMOTE system will also remove these mappings.
Do you wish to continue the 'remotepeer rm' operation (y/n): y All
attribute values for that have been changed will now be saved.
```

Reset Factory Command

Restores the router configuration parameters to the factory default values. It deletes all LUN mappings, as well as all persistent data regarding targets, LUNs, and initiators. It also restores the factory default IP addresses.

Authority Admin session

Syntax **reset**

factory

Keywords **factory**

Restores the router to factory default configuration.

Examples **Reset command example:**

```
QRouter (admin) #> reset factory

Are you sure you want to restore to factory default settings (y/n): y
Please reboot the System for the settings to take effect.
```

Save Command

Saves logs and traces.

Authority Admin session

Syntax **save**

capture
logs
traces

Keywords **capture**

The save capture command creates a debug file that captures all debug dump data. After the command completes, you must ftp the debug capture file from the router.

logs

The save logs command creates a tar file containing the router's log data, storing the file in the router's /var/ftp directory. After the command completes, you must ftp the log's tar file from the router.

traces

The save traces command creates a tar file containing the router's dump data, storing the tar file in the router's /var/ftp directory. After the command completes, you must ftp the trace's tar file from the router. If the router does not have any dump data, you will be notified when executing this command. The system creates an event log entry whenever it generates dump data.

Examples **Save capture command example:**

```
QRouter (admin) #> save capture

Debug capture completed. Package is System_Capture.tar.gz

Please use FTP to extract the file out from the System.
```

Save logs command example:

```
QRouter (admin) #> save logs

Save Event Logs completed. Package is Router_Evl.tar.gz

Please use FTP to extract the file out from the System.
```

Two Save traces command examples:

```
QRouter (admin) #> save traces

Save ASIC Traces completed. Package is Router_Asic_Trace.tar.gz

Please use FTP to extract the file out from the System.

QRouter (admin) #> save traces
No ASIC trace files exist to save. Command aborted.
```

Set Command

Configures general router parameters as well as parameters that are specific to the Fibre Channel, iSCSI, and management ports.

Authority Admin session

Syntax **set**

chap
fc [port_num]
features
Iscsi [port_num]
Isns [port_num]
mgmt
ntp
properties
snmp
system

Keywords **chap**

Sets the CHAP secrets.

fc [port_num]

Sets the Fibre Channel port parameters.

features

Sets licensed router features such as SmartWrite or additional host ports.

iscsi [port_num]

Sets the iSCSI port parameters.

isns [port_num]

Sets the iSNS parameters.

mgmt

Sets the management port parameters.

ntp

Sets the network time protocol (NTP) parameters.

properties

Sets CLI properties.

snmp

Sets the simple network management protocol (SNMP) parameters.

system

Sets system parameters such as symbolic name and log level.

Set CHAP Command

Configures general router parameters.

Authority Admin session

Syntax **set chap**

Examples **Set CHAP command example:**

```
QRouter (admin) #> set chap

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0
iqn.2004-08.com.qlogic.isr-6142.0539A01064.0.2000002037fd8bab.2200002
037fd8bab
1
iqn.2004-08.com.qlogic.isr-6142.0539A01064.1.2000002037fd8bab.2200002
037fd8bab

Please select a presented target from the list above ('q' to quit): 0

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

CHAP (0=Enable, 1=Disable) [Disabled]

All attribute values for that have been changed will now be saved.
```

Set FC Command

Configures a Fibre Channel port.

Authority Admin session

Syntax **set fc [port_num]**

Keywords **[port_num]**

The number of the FC port to be configured.

Examples **Set FC command example:**

```
QRouter (admin) #> set fc 1

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

WARNING:
The following command might cause a loss of connections to both ports.

Configuring FC Port: 1
-------------------------
Port Status (0=Enable, 1=Disable) [Enabled ]
Link Rate (0=Auto, 1=1Gb, 2=2Gb, 4=4Gb) [Auto ]
Frame Size (0=512B, 1=1024B, 2=2048B) [2048 ]
Execution Throttle (Min=16, Max=256) [64 ]
Programmed Connection Option:
(0=Loop Only, 1=P2P Only, 2=Loop Pref) [Loop Pref ]

All attribute values for Port 1 that have been changed will now be
saved.
```

Set Features Command

The set features command lets you enter licensed router features such as SmartWrite or additional host ports.

NOTE:

The date and time must be set prior to entering feature license keys.

Authority Admin session

Syntax **set features**

Examples **Set Features command example:**

```
QRouter (admin) #> set features

A list of attributes with formatting and current values will follow.

Enter a new value or simply press the ENTER key to accept the current
value.
If you wish to terminate this process before reaching the end of the
list press 'q' or 'Q' and the ENTER key to do so. Enter feature key to
be saved/activated: 1-LCWC6XKAFKC7S-SMART_WRITE

Please reboot the system for these changes to take effect.
```

Set iSCSI Command

Configures an iSCSI port.

Authority Admin session

Syntax **set iscsi [port_num]**

Keywords **[port_num]**

The number of the iSCSI port to be configured.

Examples **Set iSCSI command example:**

```
QRouter (admin) #> set iscsi 1

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

  WARNING:
  The following command might cause a loss of connections to both
ports.

  Configuring iSCSI Port: 1
  ---------------------------
  Port Status (0=Enable, 1=Disable)           [Enabled         ]
  IP Address                                  [0.0.0.0         ]
  Subnet Mask                                 [0.0.0.0         ]
  Gateway IP Address                          [0.0.0.0         ]
  Target TCP Port No. (Min=1024, Max=65535)   [3260            ]
  MTU Size (0=Normal, 1=Jumbo, 2=Other)       [Normal          ]
  Window Size (0=8KB, 1=16KB, 2=32KB)         [32768           ]
  Window Scaling (0=Enable, 1=Disable)        [Enabled         ]
  Window Scaling Factor (Min=0, Max=5)        [1               ]
  Port Speed (0=Auto, 1=100Mb, 2=1Gb)         [Auto            ]
  Header Digests (0=Enable, 1=Disable)        [Enabled         ]
  Data Digests (0=Enable, 1=Disable)          [Enabled         ]
  VLAN (0=Enable, 1=Disable)                  [Disabled        ]
  IPv6 Address 1                              [::              ]
2001::1234
  IPv6 Address 2                              [::              ]
  IPv6 Default Router                         [::              ]
```

```
  IPv6 Tgt TCP Port No. (Min=1024, Max=65535) [3260            ]
  IPv6 Window Scaling (0=Enable, 1=Disable)   [Enabled         ]
  IPv6 Window Scaling Factor (Min=0, Max=5)   [1               ]
  IPv6 VLAN (0=Enable, 1=Disable)             [Disabled        ]

All attribute values for Port 1 that have been changed will now be
saved.
```

Set iSNS Command

Configures iSNS parameters for an iSCSI port.

Authority Admin session

Syntax **set isns [port_num]**

Keywords **[port_num]**

The number of the iSCSI port to be configured for iSNS.

Examples **Set iSNS command example:**

```
QRouter (admin) #> set isns 1

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Configuring iSNS iSCSI Port: 1
--------------------------------
iSNS (0=Enable, 1=Disable)   [Disabled        ] 0
iSNS Address (IPv4 or IPv6)  [0.0.0.0         ]
fe80::21b:21ff:fe06:d517
TCP Port No.                 [3205            ]

All attribute values for Port 1 that have been changed will now be
saved.
```

Set Mgmt Command

Configures the router's management port (10/100).

Authority Admin session

Syntax **set mgmt**

Examples **Set Mgmt command example:**

```
QRouter (admin) #> set mgmt

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

  WARNING:
The following command might cause a loss of connections to the MGMT
port.

  IPv4 Interface (0=Enable, 1=Disable)[Enabled ]
  IPv4 Mode (0=Static, 1=DHCP, 2=Bootp, 3=Rarp)[Dhcp ]
  IPv6 Interface (0=Enable, 1=Disable)[Enabled ]
  IPv6 Mode (0=Manual, 1=AutoConfigure)[Manual ] 1

  All attribute values that have been changed will now be saved.
```

Set NTP Command

Use the set NTP command to configure the network time protocol parameters. NTP sets the date and time on the router from a network time server.

Authority Admin session

Syntax **set ntp**

Examples **Set NTP command example:**

```
QRouter (admin) #> set ntp

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

NTP (0=Enable, 1=Disable) [Enabled ]
TimeZone Offset from GMT (Min=-12hrs,Max=12hrs) [-8 ]
IP Address [0] [0.0.0.0 ] 207.126.97.57
IP Address [1] [0.0.0.0 ]
IP Address [2] [0.0.0.0 ]

All attribute values that have been changed will now be saved.
```

Set Properties Command

Configures the CLI (command line interface) properties.

Authority Admin session

Syntax **set properties**

Examples **Set Properties command example:**

```
QRouter (admin) #> set properties

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

CLI Inactivty Timer (0=Disable, 1=15min, 2=60min) [Disabled]
CLI Prompt (Max=32 Characters) [QRouter ] RTR1
All attribute values that have been changed will now be saved.
```

Set SNMP Command

Configures the general simple network management protocol (SNMP) properties, as well as configuring eight trap destinations.

Authority Admin session

Syntax **set snmp**

trap_destinations

Keywords **trap_destinations**

Specifies the setting of the trap destinations.

Examples **Set SNMP command example for setting the general properties:**

```
QRouter (admin) #> set snmp

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Configuring SNMP:
-----------------
Read Community [ ] Public
Trap Community [ ] Private
System Location [ ]
System Contact [ ]
Authentication Traps (0=Enable, 1=Disable) [Disabled ]

All attribute values that have been changed will now be saved.
```

Set SNMP command example for configuring an SNMP trap destination:

```
QRouter (admin) #> set snmp trap_destinations

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

Configuring SNMP Trap Destination 1 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ] 0
IP Address [0.0.0.0 ] 10.0.0.5
Destination Port [0 ] 1024

Trap Version [0 ] 2
Configuring SNMP Trap Destination 2 :
```

```
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 3 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 4 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 5 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 6 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 7 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
Configuring SNMP Trap Destination 8 :
-------------------------------------
Destination enabled (0=Enable, 1=Disable) [Disabled ]
All attribute values that have been changed will now be saved.
```

Set System Command

Configures the general router parameters.

Authority Admin session

Syntax **set system**

Examples **Set System command example:**

```
QRouter (admin) #> show system

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

System Symbolic Name (Max = 64 characters) [ ]
System Log Level (Min = 0, Max = 3) [0 ]
All attribute values that have been changed will now be saved.
```

Show Command

Displays router operational information.

Authority None

Syntax **show**

chap
fc [port_num]
fciproutes [link_id]
features
initiators [fc or iscsi]
iscsi [port_num]
isns [port_num]
localmaps
logs
memory
mgmt
ntp
perf [byte | init_rbyte | init_wbyte | tgt_rbyte | tgt_wbyte]
presented_initiators [fc | iscsi]
presented_targets [fc or iscsi]
properties
remotemaps
remotepeers
snmp
stats
system
targets [fc or iscsi]

Keywords **chap**

Displays Chap information.

fc [port_num]

Displays Fibre Channel port information.

fciproutes [link_id]

Displays FCIP routes in effect and their configuration parameters.

features

Displays installed licenses (port / SmartWrite).

initiators [fc or iscsi]

Displays SCSI initiator information: iSCSI or FC.

iscsi [port_num]

Displays iSCSI port information and configuration.

isns [port_num]

Displays the router's iSCSI name server (iSNS) configuration.

localmaps

Displays local mappings, FC to FC, iSCSI to FC, and FC to iSCSI.

logs

Displays contents of the router logs.

memory

Displays memory managed by router. Includes total and available.

mgmt

Displays the router's management port (10/100) configuration.

ntp

Displays the router's network time protocol (NTP) configuration.

perf

Displays router performance data.

presented_initiators

Displays initiators presented by the router.

presented_targets [fc or iscsi]

Displays targets presented by the router: FC, iSCSI, or both.

properties

Displays the router's CLI (command line interface) properties.

remotemaps

Displays all remote maps that have been configured.

remotepeers

Displays all remote peers.

snmp

Displays the router's simple network management protocol (SNMP) properties and trap configurations.

stats

Displays the router statistics, both FC and iSCSI.

system

Displays router product information including serial number, software version, hardware version, configuration, and temperature.

targets [fc or iscsi]

Displays targets discovered by the router: FC, iSCSI, or both.

Show CHAP Command

Displays CHAP configuration.

Authority None

Syntax **show chap**

Examples **Show CHAP command example:**

```
QRouter #> show chap

The following is a list of iSCSI nodes that have been configured with
CHAP 'ENABLED':

Type iSCSI Node
-------- ------------
No entires found.
```

Show FC Command

Displays Fibre Channel port information for the specified port. If you do not specify the port, it displays both ports.

Authority None

Syntax **show fc [port_num]**

Keywords **[port_num]**

The number of the FC port to display.

Examples **Show FC command example:**

```
QRouter (admin) #> show fc
FC Port Information
---------------------
FC Port 1
Port Status Enabled
Link Status Up
Current Link Rate 2Gb
Programmed Link Rate Auto
WWNN 20:00:00:c0:dd:0c:8b:e2
WWPN 21:00:00:c0:dd:0c:8b:e2
Port ID 02-02-ef
Firmware Revision No. 3.03.07
Frame Size 2048
Execution Throttle 64
Connection Mode Loop
Programmed Connection Option Loop Preferred
FC Port 2
Port Status Enabled
Link Status Up
Current Link Rate 2Gb
Programmed Link Rate Auto
WWNN 20:00:00:c0:dd:0c:8b:e3
WWPN 21:00:00:c0:dd:0c:8b:e3
Port ID 02-06-ef
Firmware Revision No. 3.03.07
Frame Size 2048
Execution Throttle 64
Connection Mode Loop
Programmed Connection Option Loop Preferred
```

Show FcipRoutes Command

Displays FCIP route(s) configuration parameters.

Authority None

Syntax **show fciproutes [link_id]**

Keywords **[link_id]**

The number of the FCIP route to be displayed (1 or 2).

Examples **Show FCIP routes command example:**

```
QRouter (admin) #> show fciproutes

  FCIP Route Information
  ----------------------
  FCIP Route                          1
  FCIP Interfaces Status              Enabled
  FCIP Link Status                    Down
  FC Port                             FC1
  GE Port                             GE1
  GE Link Status                      Up
  IPv6 Link Local                     fe80::2c0:ddff:fe0c:8be2
  IPv6 Remote Address                 fe80::21b:21ff:fe06:d517
  MTU Size                            Normal
  TCP Window Size                     32768
  Window Scaling                      Disabled
  TCP Port No                         3225
  GE Port Speed                       Auto
  FCIP Time Stamp                     Enabled
  Error Detect TimeOut                1
  Resource Allocate TimeOut           1
  Bandwidth, Mbit/sec                 1000
  VLAN                                Disabled
  FCIP SW Compression                 Disabled
```

Show Features Command

The show features command displays the licensed features that have been enabled on the router.

Authority None

Syntax **show features**

Examples **Show Features command example:**

```
QRouter (admin) #> show features

Feature Key Information
-------------------------
Key 7-LC7D9RMLD05XI-iSR-6142 (SMART-WRITE,39_HOSTS,62_HOSTS)
Date Applied Mon Jun 19 10:08:21 2007
```

Show Initiators Command

Displays SCSI initiator information for iSCSI, FC, or both.

Authority None

Syntax **show initiators**

fc
iscsi

Keywords **fc**

Specifies the display of Fibre Channel initiators.

iscsi

Specifies the display of iSCSI initiators.

Examples **Show Initiators command example:**

```
QRouter #> show initiators

Initiator Information
----------------------
Initiator Name iqn.1991-05.com.microsoft:qlogic-8qdaqlxt
Alias
IP Address 10.3.5.130
Portal No. 1
Status Logged In
```

Show iSCSI Command

Displays iSCSI information for the specified port. If you do not specify the port, this command displays both ports.

Authority None

Syntax **show iscsi [port_num]**

Keywords **[port_num]**

The number of the iSCSI port to display.

Examples **Show iSCSI port command example:**

```
QRouter (admin) #> show iscsi

  iSCSI Port Information
  ----------------------
  iSCSI Port                1
  Port Status               Enabled
  Link Status               Up
  iSCSI Base Name
iqn.2004-08.com.qlogic:isr-6142.0608a00471.0
  MAC Address               00-c0-dd-0c-8b-e2
  IP Address                0.0.0.0
  Subnet Mask               0.0.0.0
  Gateway IP Address        0.0.0.0
  Firmware Revision No.     3.00.02.44
  No. of Open Connections   0
  Target TCP Port No.       3260
  MTU Size                  Normal
  Window Size               32768
  Window Scaling            Enabled
  Window Scaling Factor     1
  Current Port Speed        1Gb/FDX
  Programmed Port Speed     Auto
  Header Digests            Enabled
  Data Digests              Enabled
  Max Burst                 262144
  Max First Burst           65536
  VLAN                      Disabled
  IPv6 Address 1            ::
  IPv6 Address 2            ::
```

```
  IPv6 Link Local            fe80::2c0:ddff:fe0c:8be2
  IPv6 Default Router        ::
  IPv6 Target TCP Port No.   3260
  IPv6 Window Scaling        Enabled
  IPv6 Window Scaling Factor 1
  IPv6 VLAN                  Disabled

  iSCSI Port                 2
  Port Status                Enabled
  Link Status                Up
  iSCSI Base Name
iqn.2004-08.com.qlogic:isr-6142.0608a00471.1
  MAC Address                00-c0-dd-0c-8b-e3
  IP Address                 0.0.0.0
  Subnet Mask                0.0.0.0
  Gateway IP Address         0.0.0.0
  Firmware Revision No.      3.00.02.44
  No. of Open Connections    0
  Target TCP Port No.        3260
  MTU Size                   Normal
  Window Size                32768
  Window Scaling             Enabled
  Window Scaling Factor      1
  Current Port Speed         1Gb/FDX
  Programmed Port Speed      Auto
  Header Digests             Enabled
  Data Digests               Enabled
  Max Burst                  262144
  Max First Burst            65536
  VLAN                       Disabled
  IPv6 Address 1             ::
  IPv6 Address 2             ::
  IPv6 Link Local            fe80::2c0:ddff:fe0c:8be3
  IPv6 Default Router        ::
  IPv6 Target TCP Port No.   3260
  IPv6 Window Scaling        Enabled
  IPv6 Window Scaling Factor 1
  IPv6 VLAN                  Disabled
```

Show iSNS Command

Displays iSNS configuration information for the specified iSCSI port. If you do not specify the port, this command displays the iSNS configuration information for both iSCSI ports.

Authority None

Syntax **show isns [port_num]**

Keywords **[port_num]**

The iSCSI port number whose iSNS configuration you want to display.

Examples **Show iSNS command example:**

```
QRouter (admin) #> show isns

  iSNS Information
  ------------------
  iSCSI Port     1
  iSNS           Enabled
  IPv6 Address   fe80::21b:21ff:fe06:d517
  TCP Port No.   3205

  iSCSI Port     2
  iSNS           Disabled
  IP Address     0.0.0.0
  TCP Port No.   3205
```

Show Localmaps Command

The show localmaps command displays all local mappings on the router. Local mappings are mappings between initiator and target devices.

Authority None

Syntax **show localmaps**

Examples **Show Localmaps command example:**

```
QRouter (admin) #> show localmaps

Local Mappings
----------------
Initiator iqn.1991-05.com.microsoft:qlogic-09sd5i4l
Target 20:00:00:20:37:fd:9c:f7,22:00:00:20:37:fd:9c:f7
Initiator Port GE2
Target Port FC1
Initiator 20:01:00:e0:8b:28:5f:3d,21:01:00:e0:8b:28:5f:3d
Target 20:00:00:00:87:1d:fa:64,22:00:00:00:87:1d:fa:64
Initiator Port FC2
Target Port FC2
```

Show Logs Command

Displays the router event log.

Authority None

Syntax **show logs**

Examples **Show Logs command example:**

```
QRouter #> show logs

01/01/2008 00:00:13 System 3 Tuesday 01 January 12:13 AM
01/01/2008 00:00:21 QL4022 3 #0: QLIsrDecodeMailbox: Link up
01/01/2008 00:00:13 System 3 Tuesday 01 January 12:13 AM
01/01/2008 00:00:22 QL4022 3 #0: QLIsrDecodeMailbox: Link up
```

Show Memory Command

Displays the router's memory usage. If there are no configured FCIP routes, it shows the FCIP memory usage of zero.

Authority None

Syntax **show memory**

Examples **Show Memory command example with no FCIP routes configured:**

```
QRouter #> show memory

Memory Units Free/Total
-------------- ----------
Physical 15MB/505MB
Buffer Pool 11520/12544
Process Blocks 8192/8192
Request Blocks 8192/8192
Event Blocks 1024/1024
Control Blocks 256/256
FCIP Buffer Pool 0/0
FCIP Request Blocks 16384/16384
```

Show Memory command example with one FCIP route configured:

```
QRouter #> show memory
Memory Units Free/Total
-------------- ----------
Physical 28MB/251MB
Buffer Pool 2176/4224
Process Blocks 4096/4096
Request Blocks 4096/4096
Event Blocks 512/512
Control Blocks 128/128
FCIP Buffer Pool 13320/16384
FCIP Request Blocks 15368/16384
```

Show Mgmt Command

Displays the router's management port (10/100) configuration.

Authority None

Syntax **show mgmt**

Examples **Show Mgmt command example:**

```
QRouter (admin) #> show mgmt

  Management Port Information
  ---------------------------
  IPv4 Interface           Enabled
  IPv4 Mode                Dhcp
  IPv4 IP Address          172.17.137.129
  IPv4 Subnet Mask         255.255.254.0
  IPv4 Gateway             172.17.136.1
  IPv6 Interface           Disabled
  Link Status              Up
  MAC Address              00-c0-dd-0c-8b-e1
```

Show NTP Command

Displays the router's network time protocol (NTP) configuration.

Authority None

Syntax **show ntp**

Examples **Show NTP command example:**

```
QRouter #> show ntp

NTP Information
-----------------
Mode Disabled
Status Offline
TimeZone Offset (Hours) 0
```

Show Performance Command

Displays router performance data.

Authority None

Syntax **show perf**

byte
init_rbyte
init_wbyte
tgt_rbyte
tgt_wbyte

Keywords **byte**

Displays data transfer rate of each port (FC and GE).

init_rbyte

Displays initiator read transfer rate per port.

init_wbyte

Displays initiator write transfer rate per port.

tgt_rbyte

Displays target read transfer rate per port.

tgt_wbyte

Displays target write transfer rate per port.

Examples **Show Performance (all) command example:**

```
QRouter #> show perf

Port Bytes/s Bytes/s Bytes/s Bytes/s Bytes/s
Number (init_r) (init_w) (tgt_r) (tgt_w) (total)
------ -------- -------- -------- -------- --------
GE1 0 0 22M 26M 48M
GE2 0 0 49M 50M 99M
FC1 50M 52M 0 0 103M
FC2 20M 28M 0 0 49M
```

Show Performance byte command example:

```
QRouter #> show perf byte

Displaying bytes/sec (total)... (Press any key to stop display)
GE1 GE2 FC1 FC2
------------------------------
47M 93M 94M 48M
47M 94M 96M 47M
46M 96M 96M 47M
45M 94M 97M 48M
47M 92M 93M 48M
45M 93M 94M 46M
```

Show Presented Initiators Command

Displays initiators presented by the router: FC.

Authority None

Syntax **show presented_initiators**

Examples **Show Presented Initiators command example:**

```
QRouter #> show presented_initiators

Presented Initiator Information
--------------------------------
FC Presented Initiators
------------------------
WWNN 20:01:00:c0:dd:0c:8b:e3
WWPN 21:01:00:c0:dd:0c:8b:e3
Port FC2
<MAPS TO>
WWNN 20:01:00:e0:8b:28:5f:3d
WWPN 21:01:00:e0:8b:28:5f:3d
WWNN 20:01:00:c0:dd:0c:8b:e2
WWPN 21:01:00:c0:dd:0c:8b:e2
Port FC1
<MAPS TO>
Name iqn.1991-05.com.microsoft:qlogic-09sd5i4l
```

Show Presented Targets Command

Displays targets presented by the router: FC, iSCSI, or both.

Authority None

Syntax **show presented_targets**

fc
iscsi

Keywords **fc**

Specifies the display of FC presented targets.

iscsi

Specifies the display of iSCSI presented targets.

Examples **Show Presented Targets command example where the interface is not specified:**

```
QRouter #> show presented_targets
Presented Target Information
----------------------------
FC Presented Targets
--------------------
WWNN 20:01:00:c0:dd:0c:8b:e3
WWPN 21:01:00:c0:dd:0c:8b:e3
Port FC2
<MAPS TO>
WWNN 20:00:00:00:87:1d:fa:64
WWPN 22:00:00:00:87:1d:fa:64
iSCSI Presented Targets
-----------------------
Name
iqn.2004-08.com.qlogic:isr-6142.0608a00471.1.2200002037fd9cf7.2000002
037fd9cf7
Port GE2
<MAPS TO>
WWNN 20:00:00:20:37:fd:9c:f7
WWPN 22:00:00:20:37:fd:9c:f7
```

The following is an example of the Show Presented FC Targets command:

```
QRouter #> show presented_targets fc
No Presented Targets found.
```

Show Presented iSCSI Targets command example:

```
QRouter #> show presented_targets iscsi

Presented Target Information
----------------------------
iSCSI Presented Targets
-------------------------
Name
iqn.2000-04.com.qlogic:isr6142:0.50001fe150069d20.50001fe150069d2c
IP 10.3.5.66
<MAPS TO>
WWNN 50:00:1f:e1:50:06:9d:20
WWPN 50:00:1f:e1:50:06:9d:2c
Name
iqn.2000-04.com.qlogic:isr6142:1.50001fe150069d20.50001fe150069d2c
IP 10.3.5.67
<MAPS TO>
WWNN 50:00:1f:e1:50:06:9d:20
WWPN 50:00:1f:e1:50:06:9d:2c
Name
iqn.2000-04.com.qlogic:isr6142:0.50001fe150011150.50001fe150011158
IP 10.3.5.66
<MAPS TO>
WWNN 50:00:1f:e1:50:01:11:50
WWPN 50:00:1f:e1:50:01:11:58
Name
iqn.2000-04.com.qlogic:isr6142:1.50001fe150011150.50001fe150011158
IP 10.3.5.67
<MAPS TO>
WWNN 50:00:1f:e1:50:01:11:50
WWPN 50:00:1f:e1:50:01:11:58
```

Show Properties Command

Displays the router's CLI (command line interface) properties.

Authority None

Syntax **show properties**

Examples **Show Properties command example:**

```
QRouter #> show properties

CLI Properties
----------------
Inactivty Timer Disabled
Prompt String QRouter
```

Show Remotemaps Command

Displays all remote maps that have been configured.

Authority None

Syntax **show remotemaps**

Examples **Show Remotemaps command example:**

```
QRouter #> show remotemaps

Remote Mappings
-----------------
Local Device 20:01:00:e0:8b:28:5f:3d,21:01:00:e0:8b:28:5f:3d
(Initiator)
Remote Device 20:00:00:14:c3:3d:d2:bf,22:00:00:14:c3:3d:d2:bf
(Target)
Local Port FC2
FC1
Remote System iSR-6142.0608A00471(172.17.137.143)
Status Online
Smart-Write Enabled
Compression Disabled
Load Balance Disabled
```

Show Remotepeers Command

The show remotepeers commands displays all remote peers.

Authority None

Syntax **show remotepeers**

Examples **Show Remotepeers command example:**

```
QRouter #> #> show remotepeers

Remote System Information
-------------------------
Product Name iSR-6142
Symbolic Name
Serial Number 0608A00487
HW Version 3
SW Version 2.2.0.4
No. of iSCSI Ports 2
iSCSI Base Name iqn.2004-08.com.qlogic:isr-6142.0608a00487
Mgmt IP Address 172.17.137.215
iSCSI Port 1 IP Address 10.3.5.103
iSCSI Port 1 TCP Port No. 3260
iSCSI Port 2 IP Address 10.3.5.104
iSCSI Port 2 TCP Port No. 3260
```

Show SNMP Command

Displays the router's simple network management protocol (SNMP) and any configured traps.

Authority None

Syntax **show snmp**

Examples **Show SNMP command example:**

```
QRouter #> show snmp

SNMP Configuration
------------------
Read Community Public
Trap Community Private
System Location
System Contact
Authentication traps Disabled
System OID 1.3.6.1.4.1.3873.1.5
System Description iSR-6142
Trap Destination 1
------------------
IP Address 10.0.0.5
Trap Port 1024
Trap Version 2
```

Show Stats Command

Displays the router statistics: FC and iSCSI.

Authority None

Syntax **show stats**

Examples **Show Statistics command example:**

```
QRouter #> show stats

FC Port Statistics
--------------------
FC Port 1
Interrupt Count 23
Target Command Count 0
Initiator Command Count 0
FC Port 2
Interrupt Count 1717443350
Target Command Count 0
Initiator Command Count 1815115822
iSCSI Port Statistics
-----------------------
iSCSI Port 1
Interrupt Count 3108358287
Target Command Count 1815115673
Initiator Command Count 0
MAC Xmit Frames 54392137663
MAC Xmit Byte Count 61199467593726
MAC Xmit Multicast Frames 0
MAC Xmit Broadcast Frames 0
MAC Xmit Pause Frames 0
MAC Xmit Control Frames 0
MAC Xmit Deferrals 0
MAC Xmit Late Collisions 0
MAC Xmit Aborted 0
MAC Xmit Single Collisions 0
MAC Xmit Multiple Collisions 0
MAC Xmit Collisions 0
MAC Xmit Dropped Frames 0
MAC Xmit Jumbo Frames 0
MAC Rcvd Frames 42061498217
MAC Rcvd Byte Count 60362392962831
MAC Rcvd Unknown Control Frames 0
MAC Rcvd Pause Frames 0
MAC Rcvd Control Frames 0
MAC Rcvd Dribbles 0
MAC Rcvd Frame Length Errors 0
MAC Rcvd Jabbers 0
```

```
MAC Rcvd Carrier Sense Errors 0
MAC Rcvd Dropped Frames 0
MAC Rcvd CRC Errors 0
MAC Rcvd Encoding Errors 0
MAC Rcvd Length Errors Large 1
MAC Rcvd Small Errors Small 0
MAC Rcvd Multicast Frames 34394
MAC Rcvd Broadcast Frames 33144
iSCSI Port 2
Interrupt Count 51604
Target Command Count 0
Initiator Command Count 0
MAC Xmit Frames 0
MAC Xmit Byte Count 0
MAC Xmit Multicast Frames 0
MAC Xmit Broadcast Frames 0
MAC Xmit Pause Frames 0
MAC Xmit Control Frames 0
MAC Xmit Deferrals 0
MAC Xmit Late Collisions 0
MAC Xmit Aborted 0
MAC Xmit Single Collisions 0
MAC Xmit Multiple Collisions 0
MAC Xmit Collisions 0
MAC Xmit Dropped Frames 0
MAC Xmit Jumbo Frames 0
MAC Rcvd Frames 186
MAC Rcvd Byte Count 39260
MAC Rcvd Unknown Control Frames 0
MAC Rcvd Pause Frames 0
MAC Rcvd Control Frames 0
MAC Rcvd Dribbles 0
MAC Rcvd Frame Length Errors 0
MAC Rcvd Jabbers 0
MAC Rcvd Carrier Sense Errors 0
MAC Rcvd Dropped Frames 0
MAC Rcvd CRC Errors 0
MAC Rcvd Encoding Errors 0
MAC Rcvd Length Errors Large 0
MAC Rcvd Small Errors Small 0
MAC Rcvd Multicast Frames 94
MAC Rcvd Broadcast Frames 91
iSCSI Shared Statistics
-----------------------
PDUs Xmited 2729500577
Data Bytes Xmited 55036896842234
PDUs Rcvd 2655246170
Data Bytes Rcvd 0
I/O Completed 1815115669
```

```
Unexpected I/O Rcvd 0
iSCSI Format Errors 0
Header Digest Errors 0
Data Digest Errors 0
Sequence Errors 0
PDU Xmit Count 2729500577
PDU Xmit Count 2729500577
PDU Xmit Count 2729500577
IP Xmit Packets 54392134283
IP Xmit Byte Count 59132566295008
IP Xmit Fragments 0
IP Rcvd Packets 42061430681
IP Rcvd Byte Count 58764046068744
IP Rcvd Fragments 0
IP Datagram Reassembly Count 0
IP Error Packets 0
IP Fragment Rcvd Overlap 0
IP Fragment Rcvd Out of Order 0
IP Datagram Reassembly Timeouts 0
TCP Xmit Segment Count 54392134284
TCP Xmit Byte Count 57389353022514
TCP Rcvd Segment Count 42061430681
TCP Rcvd Byte Count 57418079800284
TCP Persist Timer Expirations 0
TCP Rxmit Timer Expired 116
TCP Rcvd Duplicate Acks 986657165
TCP Rcvd Pure Acks 816265831
TCP Xmit Delayed Acks 3584507
TCP Rcvd Pure Acks 177811024
TCP Rcvd Segment Errors 0
TCP Rcvd Segment Out of Order 1
TCP Rcvd Window Probes 0
TCP Rcvd Window Updates 18500272
TCP ECC Error Corections 0
```

Show System Command

Displays router product information including the serial number, software version, hardware version, configuration, and temperature.

Authority None

Syntax **show system**

Examples **Show System command example:**

```
QRouter #> show system

  System Information
  ------------------
  Product Name                    iSR-6142
  Symbolic Name
  Serial Number                   0608A00471
  HW Version 5                    (IPv6 Supported)
  SW Version                      2.4.2.0rc2
  No. of FC Ports                 2
  No. of iSCSI Ports              2
  Temperature (C)                 31
```

Show Targets Command

Displays targets the router discovered: FC, iSCSI, or both.

Authority None

Syntax **show targets**

fc
iscsi

Keywords **fc**

Specifies the display of FC targets.

iscsi

Specifies the display of iSCSI targets.

Examples **Show FC Targets command example:**

```
QRouter #> show targets fc

Target Information
--------------------
WWNN 50:00:1f:e1:50:01:11:50
WWPN 50:00:1f:e1:50:01:11:58
Port ID 01-0d-00
Portal No. 1
State Online
WWNN 50:00:1f:e1:50:06:9d:20
WWPN 50:00:1f:e1:50:06:9d:2c
Port ID 01-08-00
Portal No. 1
State Online
```

Show iSCSI Targets command example:

```
QRouter #> show targets iscsi

No Targets found.
```

Show VLAN Command

Displays the router's VLAN configuration.

Authority None

Syntax **show vlan [port_num]**

Keywords **[port_num]**

The iSCSI port number whose VLAN configuration you want to display.

Examples **Show VLAN command example:**

```
QRouter #> show vlan

VLAN Information
------------------
Port 1
VLAN Disabled
ID 0
Priority 0
Port 2
VLAN Disabled
ID 0
Priority 0
QRouter #> show vlan 1
VLAN Information
------------------
Port 1
VLAN Disabled
ID 0
Priority 0
```

Shutdown Command

The shutdown command provides for an orderly shutdown of the routers firmware. It does not power down the router.

Authority Admin session

Syntax **shutdown**

Examples **Shutdown command example:**

```
QRouter (admin) #> shutdown
```

Target Command

Removes targets from the router's database. Typically, you can use this command to remove targets from the database that are no longer connected to the router. The target add command is not currently supported.

Authority Admin session

Syntax **target**

add
rm

Keywords **add**

Not supported

rm

Remove a target from the router's target database.

Examples **Target add command example:**

```
QRouter (admin) #> target add

Command 'target add' is currently not supported.
```

Target rm (remove) command example:

```
QRouter (admin) #> target rm

Index (WWNN,WWPN/iSCSI Name)
----- ----------------------
0 20:00:00:20:37:fd:8b:ab:00:00:00:00:fc:b6:1f:fa
Please select an 'OFFLINE' Target from the list above ('q' to quit): q
Command aborted.
```

Traceroute Command

Prints the route a network packet takes to the reach the destination specified by the user.

Authority Admin session

Syntax **traceroute**

Examples **Traceroute command example:**

```
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end
of the list press 'q' or 'Q' and the ENTER key to do so.

IP Address (IPv4 or IPv6)                 [0.0.0.0] 172.17.136.18
Outbound Port (0=Mgmt, 1=GE1, 2=GE2, ...) [Mgmt   ]

Tracing route to 172.17.136.18 over a maximum of 30 hops:

1  172.17.136.18       2.3ms       0.2ms       0.2ms
Traceroute completed in 1 hops.
```

B Log Messages

Log Data

The router maintains a message log you can retrieve and review using either the command line interface or the SANsurfer Router Manager. The message log is persistent, maintained across router power cycles and reboots. The three log message categories are:

- Informational
- Error
- Fatal

The following sections describe the log message categories.

Informational Log Messages

The following sections list and describe the informational log messages by reporting module.

Application Modules

The application modules generate the informational log messages listed in Table B-1 and described following the table.

Table B-1. Application Modules—Informational Log Messages

ID	Log Message	No.
53254	System (router) Booting up	6
53357	QLBA_ProcessTpb: De-compression failed. Disabling compression temporarily	109
54274	QLFC_Login: Origin 0x%x, VP Index 0x%x, Id 0x%x	1026
54275	QLFC_Login: Port ID %.2x%.2x%.2x	1027
54276	QLFC_Login: Node Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1028
54277	QLFC_Login: Port Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1029

Table B-1. Application Modules—Informational Log Messages (Continued)

ID	Log Message	No.
54306	QLFC_Logout: Origin 0x%x, VP Index 0x%x, Id 0x%x	1058
54307	QLFC_Logout: Port ID %.2x%.2x%.2x	1059
54308	QLFC_Logout: Node Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1060
54309	QLFC_Logout: Port Name %.2x%.2x%.2x%.2x%.2x%.2x%.2x%.2x	1061
54359	QLFC_HandleTeb: FC Login. VP 0x%x	1111
54368	QLFC_CreateVirtualInitiatorObject: Maximum host (%d) limit reached.	1120
54938	QLIS_HandleTeb: UTM_EC_OPEN_CONNECTION	1690
54939	QLIS_HandleTeb: UTM_EC_CLOSE_CONNECTION or UTM_EC_CONNECTION_CLOSED	1691
54940	QLIS_HandleTeb: UTM_EC_CONNECTION_OPENED	1692
54941	QLIS_HandleTeb:iSNS Server Open Connection succeeded	1693
54943	QLIS_HandleTeb: UTM_EC_ISNS_SCN	1695
54945	QLIS_HandleTeb: UTM_EC_ISNS_CLIENT_DISCOVERED	1697
54947	QLIS_HandleTeb: UTM_EC_CLOSE_CONNECTION	1699
54948	QLIS_HandleTeb: UTM_EC_CONNECTION_CLOSED	1700
54963	QLIS_SetDdbEntryContinue:[%d:%d] Remote system connection established	1715
54986	QLIS_HandleSessionTimer: Re-enabling compression	1738
55299	QLSC_CollectBUVUIO: Freeing dead TRB: State 0x%02X, AbortReason %d, Flags 0x%02X	2051

6	Router is booting up.
109	De-compression failed and will be temporarily disabled.
1026	FC login occurred, origin xx (1 = HBA, 2 = target, 3 = initiator), VP (virtual port) xx, ID (loop ID) xx.
1027	FC login occurred with port ID xx.xx.xx.

1028	FC login occurred with WWNN xx.xx.xx.xx.xx.xx.xx.xx.
1029	FC login occurred with WWPN xx.xx.xx.xx.xx.xx.xx.xx.
1058	FC logout occurred, origin xx (1 = HBA, 2 = target, 3 = initiator), VP (virtual port) xx, ID (loop ID) x.
1059	FC logout occurred with port ID xx.xx.xx.
1060	FC logout occurred with WWNN xx.xx.xx.xx.xx.xx.xx.xx.
1061	FC logout occurred with WWPN xx.xx.xx.xx.xx.xx.xx.xx.
1111	FC login event notification, VP (virtual port) xx.
1120	Maximum number of support hosts dd has been reached.
1690	Event notification: iSCSI open connection request.
1691	Event notification: iSCSI close connection request or connection closed.
1692	Event notification: iSCSI connection opened.
1693	Event notification: connection opened with iSNS server.
1695	Event notification: iSNS SCN received.
1697	Event notification: iSNS client discovered.
1699	iSCSI close connection request received.
1700	iSCSI connection closed.
1715	Remote system connection established using DDB d:d.
1738	Re-enabling compression.
2051	TRB freed, State xx, Abort Reason d, Flags xx.

iSCSI Driver

The following informational log messages are common to both iSCSI ports: 1 (GE1) and 2 (GE2). The messages are listed in Table B-2 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1) and log messages beginning with #1 denote iSCSI port 2 (GE2).

Table B-2. iSCSI Driver—Informational Log Messages

ID	Log Message	No.
86343	#%d: QLPortUp: Set link configuration 0x%x	327
86347	#%d: QLDisable: Restart RISC	331
86349	#%d: QLEnable: Restart RISC to update EEPROM	333
86352	#%d: QLPortDown: Set link configuration 0x%x	336
86874	#%d: QLIsrDecodeMailbox: Link up	858

327	iSCSI port enabled, port up.
331	Restart iSCSI processor (RISC).
333	EEPROM updated, restart iSCSI processor (RISC).
336	iSCSI port disabled, port down.
858	Link up reported by iSCSI processor for GE1 or GE 2.

Fibre Channel Driver

The following informational log messages are common to both Fibre Channel ports: 1 (FC1) and 2 (FC2). The messages are listed in Table B-3 and described following the table. Log messages beginning with #0 denote fibre channel port 1 (FC1). Log messages beginning with #1 denote fibre channel port 2 (FC2).

Table B-3. Fibre Channel Driver—Informational Log Messages

ID	Log Message	No.
118882	#%d: QLIoctlDisable: Reset adapter	98
119088	#%d: QLIsrEventHandler: LIP occurred (%x): mailbox1 = %x	304
119089	#%d: QLIsrEventHandler: LIP reset occurred (%x): mailbox1 = %x	305
119090	#%d: QLIsrEventHandler: Link up (%x) mailbox1 = %x	306
119092	#%d: QLIsrEventHandler: Link mode up (%x): RunTimeMode=%x	308
119093	#%d: QLIsrEventHandler: RSCN update (%x) rscnInfo: %x	309
119097	#%d: QLIsrEventHandler: Port update (%x) mb1-3 %x %x %x	313
119552	#%d: QLFcipIsrEventHandler: Link up (%x) mailbox1 = %x	768
119553	#%d: QLFcipIsrEventHandler: Link down (%x)	769
119554	#%d: QLFcipIsrEventHandler: Link mode up (%x)	770

98	Request to reset the FC processor (adapter) received from IOCTL interface.
304	Fibre Channel loop initialization procedure (LIP) occurred. The LIP type is reported, as is the contents of the FC processor's mailbox 1 register.
305	Fibre Channel LIP reset occurred. The LIP reset type is reported, as is the contents of the FC processor's mailbox 1 register.
306	Fibre Channel link up occurred. Event status is reported, as is the contents of the FC processor's mailbox 1 register.
308	Fibre Channel link up occurred. Event status is reported, as is the RunTimeMode (0 = loop, 1 = point-to-point).
309	A RSCN was received. Event status is reported, as is the RSCN information.
313	Fibre Channel port update. Event status is reported, as is the contents of the FC processor's mailbox 1, 2, and 3 registers.

768	FCIP - Fibre Channel link up occurred. Event status is reported, as is the contents of the FC processor's mailbox 1 register.
769	FCIP - Fibre Channel link down occurred.
770	FCIP - Fibre Channel link up occurred. Event status is reported, as is the RunTimeMode (0 = loop, 1 = point-to-point).

User Modules

The user modules generate the log messages listed in Table B-4 and described in the following table.

Table B-4. User Modules—Informational Log Messages

ID	Log Message	No.
151842	FW Upgrade performed: new version is: %d.%d.%d.%d	290
151843	REBOOT/SHUTDOWN Command from user. Code=%d	291
151889	#%d: qapisetfcinterfaceparams_1_svc: FC port configuration changed	337
151890	#%d: qapisetiscsiinterfaceparams_1_svc: iSCSI port configuration changed	338
151891	#%d: qapisetisns_1_svc:iSNS configuration changed	339
151892	qapisetntpparams_1_svc: NTP configuration changed	340
151893	#%d: qapisetvlanparams_1_svc: VLAN configuration changed	341
151896	qapisetmgmintfcparams_1_svc:Management port configuration changed	344
151897	qapisetbridgebasicinfo_1_svc:Bridge configuration changed	345
151898	qapimapremote_1_svc: Remotemap added for local device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	346
151899	qapimapremote_1_svc: Remotemap added to remote device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	347
151900	qapiunmapremote_1_svc: Remotemap removed for local device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	348
151901	qapiunmapremote_1_svc: Remotemap removed to remote device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	349
151902	qapimaptargettoinitiator_1_svc: Localmap added for initiator %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	350

Table B-4. User Modules—Informational Log Messages (Continued)

ID	Log Message	No.
151903	qapimaptargettoinitiator_1_svc: Localmap added to target device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	351
151904	qapiunmaptargettoinitiator_1_svc: Localmap removed for initiator device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	352
151905	qapiunmaptargettoinitiator_1_svc: Localmap removed to target device %.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x:%.2x	353
151906	qapimaptargettoinitiator_1_svc: Localmap added for initiator %s	354
151907	qapiunmaptargettoinitiator_1_svc: Localmap removed for initiator %s	355
151908	GE%d: Port status changed by user to ENABLED.	356
151909	GE%d: Port status changed by user to DISABLED.	357
151910	FC%d: Port status changed by user to ENABLED.	358
151911	FC%d: Port status changed by user to DISABLED.	359
152069	qapisetfcipparams_1_svc: FCIPROUTE %d Added	517
152070	qapisetfcipparams_1_svc: FCIPROUTE %d Modified	518
152071	qapisetfcipparams_1_svc: FCIPROUTE %d Removed	519

290	Performed router firmware upgrade, new version number is d.d.d.d.
291	User performed a router reboot or shutdown.
337	FC port configuration has been modified.
338	iSCSI port configuration has been modified.
339	iSNS configuration has been modified.
340	NTP configuration has been modified.
341	VLAN configuration has been modified.
344	Management ethernet port configuration has been modified.
345	Router configuration has been modified.
346	Remotemap added for local FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
347	Remotemap added for remote FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.

348	Remotemap removed for local FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
349	Remotemap removed for remote FC device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
350	Localmap added for FC initiator WWPN xx.xx.xx.xx.xx.xx.xx.xx.
351	Localmap added to FC target device WWPN xx.xx.xx.xx.xx.xx.xx.xx.
352	Localmap removed for FC initiator.
353	Localmap removed to FC target device.
354	Localmap added for iSCSI initiator "iqn.dddd-dd.ttt.ttt.ttt.....".
355	Localmap removed for iSCSI initiator "iqn.dddd-dd.ttt.ttt.ttt.....".
356	User enabled GE port d.
357	User disabled GE port d.
358	User enabled FC port d.
359	User disabled FC port d.
517	FCIP route #d added.
518	FCIP route #d modified.
519	FCIP route #d removed.

FCIP

The FCIP module generates the informational log messages listed in Table B-5 and described following the table.

Table B-5. FCIP—Informational Log Messages

ID	Log Message	No.
184524	qlFcip_Linkchange#%d: GigE Link Down	204
184525	qlFcip_Linkchange#%d: GigE Link Up	205

204	FCIP Route GigE link d (1 or 2) is down.
205	FCIP Route GigE link d (1 or 2) is up.

TOE Driver

The TOE driver generates the informational log messages listed in Table B-6 and described following the table.

Table B-6. TOE—Informational Log Messages

ID	Log Message	No.
217350	QL3022:eth%x: Interface is down	262

262 The GigE interface d (0 or 1) used for an FCIP route is down.

System

The system modules generate the informational log messages listed in Table B-7 and described following the table.

Table B-7. System—Informational Log Messages

ID	Log Message	No.
249862	“Temperature is back to normal range %d\n"	6

6 The router temperature has returned to the normal operating range and is d (C).

Error Log Messages

The following sections list and describe the error log messages by reporting module.

Application Modules

The application modules generate the error log messages listed in Table B-8 and described following the table.

Table B-8. Application Module—Error Log Messages

ID	Log Message	No.
40967	QLBA_NullDoorbell: driver unloaded, port disabled	7
40996	QLBA_ProcessTrb: Processing unsupported ordered tag command	36
41004	QLBA_ProcessTrb: Processing unsupported head of queue tag command	44
41058	QLBA_CreateTargetDeviceObject: Too many devices	98
41060	QLBA_CreateTargetNodeObject: Too many devices	100
41067	QLBA_CreateLunObject: LunObject memory unavailable	107
41077	QLBA_CreateInitiatorObject: Too many initiators	117
41096	QLBA_DisplayTargetOperationStatus: PCI Error, Status 0x%.2x	136
41106	QLBA_DisplayInitiatorOperationStatus: DMA Error, Status 0x%.2x	146
41107	QLBA_DisplayInitiatorOperationStatus: Transport Error, Status 0x%.2x	147
41111	QLBA_DisplayInitiatorOperationStatus: Data Overrun, Status 0x%.2x	151
41234	QLIS_LoginPduContinue: Operation failed. Initiator 0x%x, TPB status 0x%x	274
41238	QLKV_ValidateLoginTransitCsgNsgVersion failed (status 0x%x)	278
41257	QLIS_LoginPduContinue: Invalid initiator name. Initiator:	297
41265	QLIS_LoginPduContinue: Target not configured for Portal	305
41267	QLIS_LoginPduContinue: Target not found. Target name:	307
41268	QLIS_LoginPduContinue: Missing target name	308

Table B-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
41270	QLIS_LoginPduContinue: TSIH is 0 but InitiatorName key/value not provided	310
41272	QLIS_LoginPduContinue: CONN_STATE_IN_LOGIN, Unknown InitTaskTag	312
41283	QLIS_LoginPduContinue: TSIH 0x%x out of range	323
41284	QLIS_LoginPduContinue: Session does not exist, invalid TSIH 0x%x	324
41353	QLIS_LoginPduContinue CHAP Validation Failure	393
41354	QLIS_LoginPduContinue Unexpected CHAP key detected	394
41508	QLBI_SetPortInfo: QLUT_AllocatePortalObject failed (PortType 0x%x, PortId 0x%x)	548
41626	QLBI_GetLunInfo: INQUIRY failed, TPB status 0x%x	666
41629	QLBI_GetLunInfo: QLBI_PassthruCommand failed for INQUIRY (page code 0x83)	669
41635	QLBI_GetLunInfo: QLBI_PassthruCommand failed for READ CAPACITY	675
41636	QLBI_GetLunInfo: READ CAPACITY failed, TPB status 0x%x	676
41696	QLBI_PassthruCommandCompletion: Passthru command aborted	736
41700	QLBI_Passthru: Invalid CDB length %d bytes	740
41701	QLBI_Passthru: Invalid data length %d bytes	741
41717	QLBI_PassthruCommand: command interrupted or timed out	757
41750	QLBI_Ioctl: ERROR: Operation (0x%x) not supported in this mode	790
41768	QLBI_GetLunList: REPORT LUNS command failed	808
41769	QLBI_GetLunList: REPORT LUNS command failed with CHECK CONDITION, SCSI STATUS 0x%02X	809
41771	QLBI_GetLunList: Lun allocation failed for LunId %d	811
41994	QLFC_Login: VpIndex (%d) out of range	1034
41995	QLFC_Login: VP Index 0x%x not configured	1035
42002	QLFC_Login: Can't open connection	1042

Table B-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
42024	QLFC_Logout: No active path to device. WWPN: %.2X%.2X%.2X%.2X%.2X%.2X%.2X%.2X	1064
42027	QLFC_Logout: VP Index 0x%x not configured	1067
42068	QLFC_HandleTeb: System Error	1108
42069	QLFC_HandleTeb: Driver Fatal Error	1109
42072	QLFC_HandleTeb: FC Logout	1112
42242	QLIS_AllocateSessionObject: Out of session resources	1282
42252	QLIS_EnqueueiScsiPdu: Duplicate PDU, CmdSN %d (0x%x), dropping it	1292
42258	QLIS_InstantiateSession: Can't add Initiator to the database	1298
42404	QLIS_ProcessStartTrb: [%d] CmdSN %ld is out of range (%ld - %ld), Cdb[0] 0x%02X, DataXferLen 0x%x.	1444
42648	QLIS_HandleTeb: Driver Fatal Error	1688
42649	QLIS_HandleTeb: Unload Driver	1689
42654	QLIS_HandleTeb: iSNS Connection Failed	1694
43012	QLSC_CollectBUVUIO: Allocation of DSD failed	2052
43013	QLSC_CollectBUVUIORecover: Allocation of DSD failed	2053
43265	QLUT_AllocateTpbExtension: TPB allocation failed	2305
43267	QLUT_AllocateTpbExtension: Data buffer allocation failed (length %d)	2307
43268	QLUT_AllocateTpbExtension: Alloc of DSD failed for buffer len %d	2308
43269	QLFCIP_IncomingFrame: BUGCHECK: Trb (0x%p) ValidFlag (0x%x) Direction (0x%x)	2309
43270	QLFCIP_IncomingFrame: GetFcipMapPortal failed	2310
43271	QLFCIP_IncomingFrame: Got Status aborted pTrb->pBufDescList[0]:%p Trb Direction:0x%x	2311
43272	QLFCIP_SystemError: System error	2312
43273	QLFCIP_SystemError: QLOP_IssuePortEnable failed	2313

Table B-8. Application Module—Error Log Messages (Continued)

ID	Log Message	No.
43280	QLFCIP_HandleTeb: Driver Fatal error	2320
43281	QLFCIP_ConfigPortal: Find portal object failed for QLUT_TYPE_FC, PortId (%d)	2321
43282	QLFCIP_ConfigPortal: QLFCIP_ConfigPortal: Invalid PortId for FCIP link PortID(%d)	2322
43283	QLUT_AllocateFcipTrbPool: Allocation failed (size 0x%x))	2323
43284	QLUT_GetFcipTrb: Null portal object in map table	2324
43285	QLUT_GetFcipTrb: Unable to get the Free Trb	2325
43286	QLUT_GetFcipTrb: Duplicate allocation of FcipTrb (0x%p)	2326
43287	QLUT_FreeFcipTrb: Null portal object in map table	2327
43288	QLUT_FreeFcipTrb: Duplicate Free of FcipTrb (0x%p)	2328
43289	QLUT_InitializeFcipBufDescPool: Memory allocation for FCIP_BUF_EXT_DESC failed (size 0x%x)	2329
43296	QLUT_FreeFcipDataBuffers: Duplicate Freeing of DataBuf (0x%p)	2336
43297	QLUT_AllocateFcipDataBuffers: Duplicate allocation of DataBuffer (0x%p)	2337
43298	QLUT_AllocateFcipDataBuffer: Got NULL PORTAL Object in map table MEM LEAK!!!!!	2338
43299	QLUT_DeallocateFcipDataBuffer: Null portal object in map table	2339
43300	QLUT_CreateFcipDataBufferpool: Allocation of 32K buffers from LargeBufferPool failed	2340
43521	QLSC_BreakupVUIOAllocPhase: TPB allocation failed	2561
43522	QLSC_BreakupVUIOAllocPhase: Data buffer and TPB allocation failed	2562

7	NULL doorbell routine for unloaded drivers. When a driver is unloaded, the doorbell routine is redirected to this NULL routine.
36	Processing unsupported ordered tag task management command.
44	Processing unsupported head-of-queue task management command.

98	Unable to create an object for the target device: exceeded the maximum number of target devices.
100	Unable to create an object for the target node: exceeded the maximum number of target devices.
107	Memory unavailable for LUN object.
117	Unable to create an object for initiator object: exceeded the maximum number of initiators.
136	Process control block status indicates that a PCI error occurred during a target operation.
146	Process control block status indicates that a DMA error occurred during an initiator operation.
147	Process control block status indicates that a transport error (protocol) occurred during an initiator operation.
151	Process control block status indicates that a data overrun error occurred during an initiator operation.
274	iSCSI login failed between receipt of PDU and request for the data segment.
278	iSCSI login failed due to unsupported version number in received login PDU.
297	iSCSI Login PDU contains invalid initiator name. The format and character set used to form the initiator name is invalid.
305	iSCSI target login was attempted to a portal (iSCSI1 or iSCSI2) on which the target is not presented.
307	iSCSI Login PDU received for a target with a target name unknown to the router.
308	iSCSI Login PDU received without a target name for a normal session.
310	iSCSI Login PDU received without an initiator name key/value.
312	iSCSI Login PDU received with an incorrect initiator task tag for a session which is partially logged in. This would occur if a login PDU other than the initial login PDU used an initiator task tag which was different than the initiator task tag provided in the initial login PDU.
323	iSCSI Login PDU was received with a TSIH out of range. This would occur if the iSCSI initiator attempting the login failed to used the TSIH value provided in the Target Login Response PDU (router is target) in subsequent login PDUs.

324	iSCSI Login PDU was received with an invalid TSIH value. The TSIH is invalid because there is no session with that TSIH value. This would occur if the iSCSI initiator attempting the login failed to used the TSIH value provided in the target login response PDU (router is target) in subsequent login PDUs.
393	CHAP validation failed during login.
394	Unexpected CHAP key.
548	Failed to allocate an object for *Set Port Info* IOCTL processing: PortType: 0 = FC, 1 = iSCSI PortId: 0 = FC1 or iSCSI1(GE1), 1 = FC2 or iSCSI2 (GE2)
666	Inquiry command failed. The Inquiry command was issued by the router as part of its discovery process.
669	Pass-Through command for Inquiry command for page 83 failed. The Inquiry command was issued by the router as part of its discovery process.
675	Pass-Through command for Read Capacity command failed. The Read Capacity command was issued by the router as part of its discovery process.
676	Read Capacity command failed. The Read Capacity command was issued by the router as part of its discovery process.
736	Pass-Through command issued by management application (such as SANsurfer Router Manager) was aborted.
740	Pass-Through command issued by management application (such as SANsurfer Router Manager) failed due to invalid CDB length.
741	Pass-Through command issued by management application (such as SANsurfer Router Manager) failed due to invalid data length.
757	Pass-Through command issued by management application (such as SANsurfer Router Manager) was interrupted or timed out.
790	IOCTL operation unsupported. Operation code provided in log message.
808	Report LUNs command failed. The Report LUNs command was issued by the router as part of its discovery process.
809	Report LUNs command failed with check condition status. The Report LUNs command was issued by the router as part of its discovery process.
811	Failed to allocate LUN object: out of resources.
1034	Login attempted using Fibre Channel virtual port (VP) index that is out-of-range (range = 0–31). Index reported in log message.
1035	Login attempted using Fibre Channel VP index that has not been configured. Operation attempted on an unconfigured VP.

1042	Attempting login but Fibre Channel connection cannot be opened.
1064	Attempting logout of device for which there is no active path (WWPN not found).
1067	Logout attempted using Fibre Channel VP index that has not been configured. Operation attempted on an unconfigured VP.
1108	Event notification: Fibre Channel processor encountered a system error (unrecoverable firmware error).
1109	Event notification: Fibre Channel driver encountered a fatal error.
1112	Event notification: Fibre Channel port logged out.
1282	Failed to allocate object for iSCSI session: out of session resources.
1292	Received iSCSI PDU with duplicate command sequence number (CmdSN). Command PDU will be dropped.
1298	Unable to allocate iSCSI initiator object while instantiating session.
1444	Failed to execute iSCSI Command PDU because its CmdSN is out-of-range. Log message contains the incorrect CmdSN, the valid CmdSN range, the first byte of the CDB, and the data length.
1688	Event notification: iSCSI driver encountered a fatal error.
1689	Event notification: an IOCTL request was received to unload the iSCSI driver.
1694	Event notification: attempt to connect to the iSNS server failed.
2052	iSNS connection failed.
2053	Break up I/O DSD allocation failed.
2305	Break up I/O recover DSD allocation failed.
2307	Data buffer allocation failed (length %d) during tpb extension allocation.
2308	Allocation of DSD failed during Tpb extension allocation. Buffer length %d.
2309	FCIP incoming frame: BUGCHECK: Trb (0x%p) ValidFlag (0x%x) Direction (0x%x).
2310	FCIP incoming frame: GetFcipMapPortal failed.
2311	FCIP incoming frame: Got Status aborted pTrb->pBufDescList[0]:%p Trb Direction:0x%x.
2312	FCIP system error.
2313	FCIP system error: QLOP_IssuePortEnable failed.

2320	FCIP handle Teb: Driver Fatal error.
2321	FCIP configure portal: Find portal object failed for QLUT_TYPE_FC, PortId (%d).
2322	FCIP configure portal: QLFCIP_ConfigPortal: Invalid PortId for FCIP link PortID(%d).
2323	FCIP allocate TRB pool: Allocation failed (size 0x%x).
2324	FCIP Trb: Null portal object in map table.
2325	FCIP eet TRB: Null portal object in map table.
2326	FCIP get TRB: Duplicate allocation of FcipTrb (0x%p).
2327	FCIP free TRB: Null portal object in map table.
2328	FCIP free TRB: Duplicate Free of FcipTrb (0x%p).
2329	FCIP initialize buffer descriptor pool: memory allocation for FCIP_BUF_EXT_DESC failed (size 0x%x).
2336	FCIP free data buffers: Duplicate Freeing of DataBuf (0x%p).
2337	FCIP allocate data buffers: Duplicate allocation of DataBuffer (0x%p).
2338	FCIP allocate data buffer: Got NULL PORTAL Object in map table MEM LEAK.
2339	FCIP de-allocate data buffer: Null portal object in map table.
2340	FCIP create data buffer pool: Allocation of 32K buffers from LargeBufferPool failed.
2561	Break up I/O: TPB allocation failed.
2562	Break up I/O: Data buffer and TPB allocation failed.

iSCSI Driver

The following error log messages are common to both iSCSI ports, 1 (GE1) and 2 (GE2). They are listed in Table B-9 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1). Log messages beginning with #1 denote iSCSI port 2 (GE2).

Table B-9. iSCSI Driver—Error Log Messages

ID	Log Message	No.
73990	#%d: QLUtmIoctlEnable: Initialize FW failed	262
74046	#%d: QLPortUp: MBOX_CMD_SET_PORT_CONFIG %04x failed %04x	318
74056	#%d: QLRunDiag: MBOX Diag test internal loopback failed %x %x	328
74057	#%d: QLRunDiag: MBOX Diag test external loopback failed %x %x	329
74065	#%d: QLPortDown: MBOX_CMD_SET_PORT_CONFIG %04x failed %04x	337
74241	#%d: QLiSNSEnableCallback: iSNS Server TCP Connect failed	513
74577	#%d: QLIsrDecodeMailbox: NVRAM invalid	849
74587	#%d: QLIsrDecodeMailbox: Link down	859
74656	#%d: QLReadyTimer: Adapter missed heartbeat for %d seconds. Time left %d	928
74661	#%d: QLTimer: Abort pTpb=%p, Type %x, Timeout 0x%x DrvCount 0x%x, DdbIndex 0x%x	933
74663	#%d: QLReadyTimer: MBOX_CMD %04x %04x %04x %04x %04x %04x %04x %04x timed out	935
74665	#%d: QLReadyTimer: QLiSNSReenable failed.	937
74784	#%d: QLUpdateInitiatorData: No more room in Initiator Database.	1056
74800	#%d: QLSetTargetData: No more room in Target Database.	1072

262	The iSCSI processor failed firmware initialization.
318	The iSCSI processor command to enable a GE port failed.
328	The iSCSI processor failed the internal loopback test.

329	The iSCSI processor failed the external loopback test.
337	The iSCSI processor command to disable a GE port failed.
513	The iSCSI processor could not connect with the iSCSI name server (iSNS).
849	The iSCSI processor reported that the iSCSI port NVRAM contains invalid data (checksum error).
859	The iSCSI processor reported a link down condition.
928	The driver failed to receive a heartbeat from the iSCSI processor for the specified number of seconds.
933	The driver timed out an iSCSI processor operation and is aborting the operation.
935	The driver timed out an iSCSI processor mailbox command.
937	The driver timed out while attempting to reconnect with the iSNS.
1056	The driver's initiator database is full. The driver is capable of storing 1024 iSCSI initiators in its database. Use the CLI or SANsurfer Router Manager to remove unwanted/unused iSCSI initiators.
1072	The driver's target database is full. Use the CLI or SANsurfer Router Manager to remove unwanted/unused iSCSI targets.

Fibre Channel Driver

The following error log messages are common to both Fibre Channel ports, 1 (FC1) and 2 (FC2). They are listed in Table B-10 and described in this section. Log messages beginning with #0 denote fibre channel port 1 (FC1) and log messages beginning with #1 denote fibre channel port 2 (FC2).

Table B-10. Fibre Channel Driver—Error Log Messages

ID	Log Messages	No.
106583	#%d: QLUtmReceiveIo: Path invalid/FW No resource count %x	87
106589	#%d: QLIoctlEnable: Adapter disabled	93
106590	#%d: QLIoctlEnable: Initialize FW error	94
106592	#%d: QLIoctlRunDiag: Diagnostic loopback command failed %x % %x %x	96
106593	#%d: QLIoctlDisable: Re-initialize adapter failed	97
106595	#%d: QLUtmReceiveIo: Invalid VP Loop Id 0x%x	99
106803	#%d: QLIsrEventHandler: Link down (%x)	307
106813	#%d: QLIsrEventHandler: Unexpected async event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	317
106846	#%d: QLProcessResponseQueueFS: TRB is NULL: %d	350
106853	#%d: QLTimer: Link error count (0x%x) exceeded, link down	357
106912	#%d: QLReserveLoopId: out of loop Ids	416
106928	#%d: QLMarkDeviceOffline: Device Id: %x marked offline, cLinkDownTimeout = %x, cPortDownRetryCount=%x	432
106948	#%d: QLSnsGetAllNext: Name server login FAILED %x	452
107029	#%d: QLUpdateDeviceData: out of slots in host database	533
107030	#%d: QLUpdateDeviceData: out of slots in target database	534
107041	#%d: QLUpdateDeviceDatabase 0x%x: GET_ID failed %x	545
107056	#%d: QLUpdateDeviceDatabase 0x%x: out of slots in host database	560
107058	#%d: QLUpdateDeviceDatabase 0x%x: MBOX_CMD_GET_VP_DATABASE failed %x	562
107078	#%d: QLUpdatePort 0x%x: out of slots in host database	582

Table B-10. Fibre Channel Driver—Error Log Messages (Continued)

ID	Log Messages	No.
107254	#%d: QLUpdateSinglePortCont 0x%x: out of slots in host database	758
107267	#%d: QLFcipIsrEventHandler: System error event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	771

87	The FC processor received a SCSI command for an unknown target path or has run out of resources to execute additional commands.
93	The FC processor was disabled by an IOCTL request to the driver.
94	The FC processor firmware failed initialization. The request to initialize was received by the driver in an IOCTL request.
96	The FC processor failed the external loopback test.
97	The FC processor failed to re-initialize in response to an IOCTL disable request.
99	Invalid Virtual Port loop ID.
307	The FC processor reported a link down condition.
317	The FC processor reported an unexpected asynchronous event. The mailbox registers provide status, event code, and data related to the event.
350	FCIP Response queue entry TRB pointer is NULL.
357	The driver has determined that the FC link is unreliable and unusable due to the number of errors encountered. The link has been taken down.
416	The FC processor was unable to obtain the number of loop IDs required. This failure occurs only when the FC processor is running multi-ID firmware.
432	The driver was unable to re-establish connection to the target within the timeout and retry counts, and is therefore marking it *offline*.
452	The FC processor is unable to log into the FC fabric name server.
533	The driver’s host (initiator) database is full.
545	The driver’s target database is full.
560	The driver’s host (initiator) database is full. Maximum host database is 64.
562	FC processor "Get VP Database entry command" failed.

582	The drivers host (initiator) database is full.
758	No slots available in host database.
771	FCIP system error event.

User Modules

The user modules generate the error log messages listed in Table B-11 and described following the table.

Table B-11. User Modules—Error Log Messages

ID	Log Message	No.
139265	QBRPC_Initialize: Entered	1
139266	QBRPC_Initialize:GetBridge Mem Allocation error	2
139267	QBRPC_Initialize:GetBridgeAdv Mem Allocation error	3
139268	QBRPC_Initialize:GetMgmt Mem Allocation error	4
139269	QBRPC_Initialize:GetIscsi Mem Allocation error	5
139270	QBRPC_Initialize:GetIscsiAdv Mem Allocation error	6
139271	QBRPC_Initialize:GetIsns Mem Allocation error	7
139272	QBRPC_Initialize:GetFcIntfc Mem Allocation error	8
139273	QBRPC_Initialize:GetFcAdv Mem Allocation error	9
139280	QBRPC_Initialize:GetFcSfp Mem Allocation error	16
139281	QBRPC_Initialize:GetLog Mem Allocation error	17
139282	QBRPC_Initialize:GetStats Mem Allocation error	18
139283	QBRPC_Initialize:InitListMem Allocation error	19
139284	QBRPC_Initialize:TargetList Mem Allocation error	20
139285	QBRPC_Initialize:LunList MemAllocation error	21
139286	QBRPC_Initialize:PresTarget Mem Allocation error	22
139287	QBRPC_Initialize:LunMask Mem Allocation error	23
139288	QBRPC_Initialize:Init Mem Allocation error	24
139289	QBRPC_Initialize:TgtDevice Mem Allocation error	25
139296	QBRPC_Initialize:FcTgt Mem Allocation error	32

Table B-11. User Modules—Error Log Messages (Continued)

ID	Log Message	No.
139297	QBRPC_Initialize:BridgeStatus Mem Allocation error	33
139298	QBRPC_Initialize:Diag Mem Allocation error	34
139299	QBRPC_Initialize:DiagLog Mem Allocation error	35
139300	QBRPC_Initialize:FruImage Mem Allocation error	36
139301	QBRPC_Initialize:OemMfg Mem Allocation error	37
139302	QBRPC_Initialize:Status Mem Allocation error	38
139303	QBRPC_Initialize:TcpIpStats Mem Allocation error	39
139304	QBRPC_Initialize:NtpStats Mem Allocation error	40
139305	QBRPC_Initialize:LunList MemAlloc error	41
139315	QBRPC_FreeResources:Entered	51
139553	checkDuplicateIp: Detected Error %08x %08x%04x	289

1	RPC (remote procedure call) server initialization entry point.
2	Get System API memory allocation failed.
3	Get System Advanced API memory allocation failed.
4	Get Management API memory allocation failed.
5	Get iSCSI API memory allocation failed.
6	Get iSCSI advanced API memory allocation failed.
7	Get iSNS API memory allocation failed.
8	Get FC Interface API memory allocation failed.
9	Get FC Advanced API memory allocation failed.
16	Failed memory allocation for Get FC SFP API.
17	Failed memory allocation for Get Log API.
18	Failed memory allocation for Get Statistics API.
19	Failed memory allocation for Get Initiator List API.
20	Failed memory allocation for Get Target List API.

21	Failed memory allocation for Get LUN List API.
22	Failed memory allocation for Get Presented Targets List API.
23	Failed memory allocation for Get LUN Mask API.
24	Failed memory allocation for Initiator API.
25	Failed memory allocation for Target Device API.
32	Failed memory allocation for FC Target API.
33	Failed memory allocation for System Status API.
34	Failed memory allocation for Diagnostic API.
35	Failed memory allocation for Diagnostic Log API.
36	Failed memory allocation for FRU Image API.
37	Failed memory allocation for OEM Manufacturing API.
38	Failed memory allocation for Status API.
39	Failed memory allocation for TCP/IP Statistics API.
40	Failed memory allocation for NTP Status API.
41	Failed memory allocation for LUN List API.
51	RPC free resources entry point.
289	Detected duplicate IP address for management port.

System

The system modules generate the error log messages listed in Table B-12 and described following the table.

Table B-12. System—Error Log Messages

ID	Log Message	No.
237572	"Failed to kill sys killer %d\n"	4
237573	"Temperature over high threshold %d\n"	5

4	Failed to kill system task.
5	Reporting router exceeds maximum operating temperature.

Fatal Log Messages

The following sections list and describe the fatal log messages by reporting module.

iSCSI Driver

The following fatal log messages are common to both iSCSI ports, 1 (GE1) and 2 (GE2). They are listed in Table B-13 and described following the table. Log messages beginning with #0 denote iSCSI port 1 (GE1). Log messages beginning with #1 denote iSCSI port 2 (GE2).

Table B-13. iSCSI Driver—Fatal Log Messages

ID	Log Message	No.
69652	#%d: qlutm_init: Diagnostic failed, invalid SRAM	20
69653	#%d: qlutm_init: Diagnostic failed, fail reboot	21
69654	#%d: qlutm_init: Diagnostic failed, invalid NVRAM	22
69655	#%d: qlutm_init: Diagnostic failed, invalid DRAM	23
69656	#%d: qlutm_init: Failed to return diagnostic result to Bridge	24
69941	#%d: QLUtmProcessResponseQueue: Invalid handle %x EntryType %x	309
69951	#%d: QLSetNvram: QLRebootTimer failed AF %x RS %x Time %d	319

Table B-13. iSCSI Driver—Fatal Log Messages (Continued)

ID	Log Message	No.
69964	#%d: QLDisable: QLRebootTimer failed AF %x RS %x Time %d	332
69966	#%d: QLEnable: QLRebootTimer failed AF %x RS %x Time %d	334
70224	#%d: QLProcSrblessiSNSResponse: Invalid handle %x	592
70400	#%d: QLInitializeDevice: QLStartAdapter failed	768
70417	#%d: QLInitializeAdapter: QLInitializeFW failed	785
70432	#%d: QLDoInterruptServiceRoutine: PortFatal interrupt. PortFatalErrorStatus %08x CSR %08x AS %x AF %x	800
70448	#%d: QLStartAdapter: QLRebootTimer failed AF %x RS %x Time %d	816
70489	#%d: QLIsrDecodeMailbox: System Error 8002 MB[1-7] %04x %04x %04x %04x %04x %04x %04x	857
70499	#%d: QLProcessResponseQueue: Invalid handle for ET_PASSTHROUGH_STATUS	867
70501	#%d: QLProcessResponseQueue: Invalid entry type in response queue %x	869
70502	#%d: QLProcessResponseQueue: Invalid handle %x EntryType %x	870
70524	#%d: QLProcessAen: Invalid event %x	892
70544	#%d: QLRebootTimer: Reboot failed!	912
70563	#%d: QLReadyTimer: Adapter missed heartbeat for 0x%x seconds. Rebooting	931
70564	#%d: QLReadyTimer: Abort pTpb=%p failed, DrvCount 0x%x	932
70609	#%d: QLProcessSystemError: Restart RISC	977
70610	#%d: QLProcessSystemError: RebootHba failed	978
70784	#%d: QLConfigChip: invalid NVRAM	1152
70835	#%d: QLStartFw: MBOX_CMD_SET_FLASH failed %x	1203
70836	#%d: QLStartFw: Invalid Fw loader state 0x%x	1204
70837	#%d: QLStartFw: Load Fw loader timeout	1205

20	iSCSI processor SRAM test failed.
21	iSCSI processor failed diagnostic reboot.
22	iSCSI processor failed NVRAM diagnostic.
23	iSCSI processor failed DRAM diagnostic.
24	iSCSI processor failed to return diagnostic results.
309	Response queue entry contains an invalid handle.
319	Set NVRAM reboot timer failed.
332	Port disable reboot timer failed.
334	Port enable reboot timer failed.
592	iSNS response contains an invalid handle.
768	Start iSCSI processor failed.
785	iSCSI processor firmware initialization failed.
800	iSCSI processor port fatal error.
816	Start iSCSI processor reboot timer failed.
857	iSCSI processor fatal system error.
867	Response queue invalid handle for ET pass-through.
869	Response queue invalid entry type.
870	Response queue invalid handle for specified entry type.
892	Asynchronous event for unknown event type.
912	Reboot timer failed.
931	iSCSI driver missed iSCSI processor heartbeat. iSCSI processor rebooted.
932	iSCSI processor failed to complete operation before timeout.
977	iSCSI processor system error restart.
978	iSCSI processor reboot failed.
1152	iSCSI processor NVRAM invalid (checksum error).
1203	iSCSI FLASH (NVRAM) command failed.
1204	iSCSI firmware loader invalid state.
1205	iSCSI failed to load firmware in time allotted.

FC Driver

The following fatal log messages are common to both Fibre Channel ports, 1 (FC1) and 2 (FC2). They are listed in Table B-14 and described following the table. Log messages beginning with #0 denote fibre channel port 1 (FC1). Log messages beginning with #1 denote fibre channel port 2 (FC2).

Table B-14. Fibre Channel Driver—Fatal Log Messages

ID	Log Message	No.
102419	#%d: qlutm_init: Diagnostic failed, port 1 invalid SRAM	19
102420	#%d: qlutm_init: Diagnostic failed, port 1 POST failed	20
102421	#%d: qlutm_init: Diagnostic failed, port 2 invalid SRAM	21
102422	#%d: qlutm_init: Diagnostic failed, port 2 POST failed	22
102423	#%d: qlutm_init: Failed to return diagnostic result to Bridge	23
102656	#%d: QLInitializeAdapter: Reset ISP failed	256
102657	#%d: QLInitializeAdapter: Load RISC code failed	257
102658	#%d: QLInitializeAdapter: Load ISP2322 receive sequencer code failed	258
102659	#%d: QLInitializeAdapter: Load ISP2322 transmit sequencer code failed	259
102662	#%d: QLInitializeAdapter: Verify Checksum command failed (%x)	262
102680	#%d: QLInitializeFW: FAILED	280
102688	#%d: QLInterruptServiceRoutine: Risc pause %x with parity error hccr %x, Disable adapter	288
102689	#%d: QLInterruptServiceRoutine: Invalid interrupt status: %x	289
10691	#%d: QLFcipInterruptServiceRoutine: Risc pause %x with parity error hccr %x, Disable adapter	291
10692	#%d: QLFcipInterruptServiceRoutine: Invalid interrupt status: %x	292
102716	#%d: QLIsrEventHandler: System error event (%x), MB1=%x, MB2=%x, MB3=%x, MB4=%x, MB5=%x, MB6=%x, MB7=%x	316
102746	#%d: QLProcessResponseQueue: Invalid handle %x, type %x	346
102747	#%d: QLProcessResponseQueueFS: Invalid buffer type: %x	347
102748	#%d: QLProcessResponseQueueFS: Invalid EntryType (0x%x)	348

Table B-14. Fibre Channel Driver—Fatal Log Messages (Continued)

ID	Log Message	No.
102749	#%d: QLProcessResponseQueueFS: Invalid handle 0x%x, type 0x%x	349
102752	#%d: QLTimer: Ext Ram parity error exceed limit cnt 0x%x, limit 0x%x, Disabled adapter	352
102755	#%d: QLTimer: Heartbeat failed	355
102800	#%d: QLRestartRisc: restart RISC	400

19	FC1 processor SRAM test failed.
20	FC1 processor power-on self-test (POST) failed.
21	FC2 processor SRAM test failed.
22	FC2 processor POST failed.
23	FC processor failed to return diagnostic results.
256	FC processor failed reset.
257	FC processor firmware load failed.
258	FC processor receive sequencer code load failed.
259	FC processor transmit sequencer code load failed.
262	FC processor firmware checksum failed.
280	FC processor firmware initialization failed.
288	FC processor paused due to internal parity error.
289	FC processor returned an invalid interrupt status.
291	FC processor invalid interrupt status.
292	FC processor paused due to RAM parity error.
316	FC processor system error.
346	Response queue entry contains an invalid handle.
347	FCIP: Response queue entry contains an invalid buffer type.
348	FCIP: Response queue entry contains an invalid entry type.
349	FCIP: Response queue entry contains an invalid handle.

352	FC processor external SRAM parity error count exceeded limit: FC port disabled.
355	FC processor heartbeat failed.
400	FC processor being restarted.

TOE Driver

The TOE driver generates the fatal log messages listed in Table B-15 and described following the table.

Table B-15. TOE—Fatal Log Messages

ID	Log Message	No.
200721	QL3022:ql3xxx_probe: Adapter eth#%d, Invalid NVRAM parameters	17
200725	QL3022:eth%x: Resetting chip. PortFatalErrStatus register = 0x%x	21

17	Encountered invalid parameters in TOE NVRAM.
21	TOE chip reset due to detection of fatal error.

System

The system modules generate the fatal log messages listed in Table B-16 and described following the table.

Table B-16. System—Fatal Log Messages

ID	Log Message	No.
233473	"memory monitor: Detected Uncorrectable Ecc %08lx system is rebooting in 5 secs\n"	1
233474	"Failed to register interrupt handler!\n"	2
233475	"%s class_simple_create failed\n"	3

1	Uncorrectable memory error detected at address provided in log message.
2	Attempt to register the interrupt handler failed.
3	Failed class_simple_create system call from memory monitor initialization routine.

Notes

C Configuring CHAP

CHAP Definition

In challenge handshake authentication protocol (CHAP), the authentication agent sends the client program a random value that is used only once and an ID value. Both the sender and peer share a predefined secret. The peer concatenates the random value, the ID, and the secret, and calculates a one-way hash using MD5 (Message-Digest algorithm 5). It sends the hash value to the authenticator, which in turn builds that same string on its side, calculates the MD5 checksum, and compares the result with the value received from the peer. If the values match, the peer is authenticated.

By transmitting only the hash, the secret cannot be reverse-engineered. The ID value is increased with each CHAP dialogue to protect against replay attacks.

Configuring CHAP Using CLI

The following sections describe the procedure for configuring CHAP from the command line interface (CLI).

CLI—Discovery Session—Bi-directional CHAP

To configure a bi-directional CHAP used during a discovery session:

1. On the router:
   a. Enable CHAP on the port.
   b. Create a secret (for example, *secret_port).*
   c. Using **Set Chap**, choose the iSCSI node that represented the GE port.
   d. Use **Show Iscsi** to find the iSCSI node name of the GE port.
2. Use **Initiator add** to add the initiator that is about to do discovery:
   a. Enable the CHAP for this initiator.
   b. Create a secret (for example, *secret_initiator*).
   c. Use **Set Chap** to update the CHAP settings of the initiator.
3. Go to the Microsoft iSCSI (MS) Initiator and perform the following steps:

a. Click **General**.

b. Click **Secret** (in the middle of the screen). If this is the first time you are setting secrets, reset all secrets.

c. Type the secret (*secret_port*) that you created in Step 1.

4. Click **Discovery**.
5. Click **Add**.
6. Type the address of the iSCSI port of the router.
7. Click **Advanced**.
8. Select **Chap Login Information**.
9. Type the secret (*secret_initiator*) you created in Step 2 into **Target Secret**.
10. Select **Mutual Authentication**.
11. Click **OK**.
12. Click **OK**. The initiator completes the discovery.

CLI—Discovery Session—Uni-directional CHAP

To configure a single-direction CHAP used during a discovery session:

1. Do not enable CHAP on the ISCSI port.
2. Use **Initiator add**:

   a. Add the initiator that is about to perform the discovery.

   b. Enable the CHAP for this initiator.

   c. Create a secret (for example, *secret_initiator*).

   d. Use **Set Chap** to update the initiator's CHAP settings.

3. Go to the MS Initiator.
4. Click **Discovery**.
5. Click **Add**.
6. Type the address of the iSCSI port of the router.
7. Click **Advanced**.
8. Select **Chap Login Information**.
9. In **Target Secret**, type the secret (*secret_initiator*) you created in Step 2.
10. Click **OK**.
11. Click **OK**. The initiator should complete discovery.

CLI—Normal Session—Bi-directional CHAP

To configure a bi-directional CHAP used during a normal session:

1. On the router
   a. Enable CHAP on the presented target to which the initiator will login.
   b. Create a secret (for example, *secret_target*).
   c. Use **Set CHAP**.
2. Use **Initiator add** to add the initiator that is about to do a normal login:
   a. Enable the CHAP for this initiator.
   b. Create a secret (for example, *secret_initiator)*.
   c. Use **Set Chap** to update the CHAP settings of the initiator.
3. Go to the MS Initiator and perform the following steps:
   a. Click **General**.
   b. Click **Secret** (in the middle of the screen).
   c. If this is the first time you are setting secrets, reset all the secrets.
   d. Type the secret (*secret_target*) that you created in Step 1.
4. Click **Targets**.
5. Select the target you want to login to.
6. Click **Advanced**.
7. Select **Chap Login Information**.
8. Type the secret *(secret_initiator*) that you created in Step 2 into **Target Secret**.
9. Select **Mutual Authentication**.
10. Click **OK.**
11. Click **OK**. The initiator completes the normal login.

CLI—Normal Session—Uni-directional CHAP

To configure single-direction CHAP to be used during a normal session:

1. Do not enable CHAP on the presented target.
2. Use **Initiator add**:
   a. Add the initiator that is about to do a normal login.
   b. Enable the CHAP for this initiator.
   c. Create a secret (for example, *secret_initiator*).
   d. Use **Set Chap** to update the CHAP settings of the initiator.
3. Go to the MS Initiator.
4. Click **Targets**.
5. Select the target you want to login to.
6. Click **Advanced**.
7. Select **Chap Login Information.**
8. Type the secret (*secret_initiator*) that you created in into **Target Secret**.
9. Click **OK**.
10. Click **OK**. The initiator completes the normal login.

Configuring CHAP Using the GUI

The following sections describe the procedure for configuring CHAP using the SANsurfer Router Manager, the graphical user interface (GUI).

GUI—Discovery Session—Bi-directional CHAP

To configure a bi-directional CHAP during a discovery session:

1. On the bridge, enable CHAP for the iSCSI port.
2. Select the port in the left column.
3. Click **Advanced Configuration**.
4. Select **Enable Chap**.
5. Type a secret in **Chap secret** (for example, *secret_port*).
6. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go to Step 10.
7. Type the IQN name string.

8. Select **Enable CHAP**.
9. Create a CHAP secret (for example, *secret_initiator*).
10. Go to the MS Initiator and perform the following steps:
    a. Click **General**.
    b. Click **Secret** (in the middle of the screen).
    c. If this is the first time you are setting secrets, reset all secrets.
    d. Type the CHAP secret (*secret_port*) that you created in Step 5.
11. Click **Discovery**.
12. Click **Add**.
13. Enter the address of the iSCSI port of the bridge.
14. Click **Advanced**.
15. Select **Chap Login Information**.
16. Type the secret (*secret_initiator*) that you created in Step 9 into **Target Secret**.
17. Select **Mutual Authentication**.
18. Click **OK**.
19. Click **OK**. The initiator completes discovery.

GUI—Discovery Session—Uni-directional CHAP

To program a single-direction CHAP during a discovery session:

1. Do not enable CHAP on the iSCSI port.
2. Check to see if the initiator exists on the discovered iSCSI initiators list:
    - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
    - If the initiator is part of the discovered list, then go to Step 6.
3. Type the IQN name string.
4. Select **Enable Chap**.
5. Create a CHAP secret (for example, *secret_initiator*).
6. Go to the MS Initiator and perform the following steps:
    a. Click **Discovery**.
    b. Click **Add**.
    c. Enter the address of the iSCSI port of the bridge.

d. Click **Advanced**.

e. Click **Chap Login Information**.

f. Type the secret (*secret_initiator*) you created in Step 5 into **Target Secret**.

7. Click **OK**.
8. Click **OK**. The initiator completes discovery.

GUI—Normal Session—Bi-directional CHAP

To program bi-directional CHAP during a normal session:

1. On the bridge, enable CHAP for the iSCSI presented target.
2. Select the presented target on the left column of the SANsurfer Router Manager.
3. Click **Information**.
4. Select **Enable Chap**.
5. Type a secret in the **Chap secret** dialog box (for example, *secret_target*).
6. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go to Step 10.
7. Fill in the IQN name string.
8. Select **Enable Chap**.
9. Create a CHAP secret (for example, *secret_initiator*).
10. Go to the MS Initiator and perform the following steps:
    a. Click **General**.
    b. Click **Secret** (in the middle of the screen).
    c. If this is the first time you are setting secrets, reset all the secrets.
    d. Type the secret (*secret_target*) that you created in Step 5.
11. Click **Targets**.
12. Select the target you want to login to.
13. Click **Log On**.
14. Click **Advanced**.
15. Select **Chap Login Information**.

16. Type the secret (*secret_initiator*) that you created in Step 9 into **Target Secret**.
17. Select **Mutual Authentication**.
18. Click **OK**.
19. Click **OK**. The initiator completes normal login.

GUI—Normal Session—Uni-directional CHAP

To program single-direction CHAP during a normal session:

1. Do not enable CHAP on the iSCSI presented target.
2. Check to see if the initiator exists on the discovered iSCSI initiators list:
   - If the initiator *is not* part of the discovered iSCSI initiators list, then go to the wizard menu and select **Add Initiator Wizard**.
   - If the initiator is part of the discovered list, then go too Step 6.
3. Fill in the IQN name string.
4. Select **Enable Chap**.
5. Create a CHAP secret (for example, *secret_initiator*).
6. Go to the MS Initiator and perform the following steps:
   a. Click **Targets**.
   b. Select the target you want to login to.
   c. Click **Log On**.
   d. Click **Advanced**.
   e. Click **Chap Login Information**.
   f. Type the secret (*secret_initiator*) you created in Step 5 into **Target Secret**,
   g. Click **OK**.
7. Click **OK**. The initiator completes normal login.

Notes

D Simple Network Management Protocol (SNMP)

Introduction

Simple network management protocol (SNMP) provides monitoring and trap functions for managing the router through third-party applications that support SNMP. The router firmware supports SNMP versions 1 and 2 and a QLogic Management Information Base (MIB). You may format the traps using SNMP version 1 or 2 (See Notifications).

SNMP Properties

You can set the SNMP properties using either the command line interface (see Set SNMP Command) or the SANsurfer Router Manager.

Table D-1 describes the SNMP properties.

Table D-1. SNMP Properties

Parameter	Description
Read community	A password that authorizes an SNMP management server to read information from the router. This is a write-only field. The value on the router and the SNMP management server must be the same. The read community password can be up to 32 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is password is *public*.
Trap community	A password that authorizes an SNMP management server to receive traps. This is a write-only field. The value on the router and the SNMP management server must be the same. The trap community password can be up to 32 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default password is *public*.
System location	Specifies the name of the router location. The name can be up to 64 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is undefined.

Table D-1. SNMP Properties (Continued)

Parameter	Description
System contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters *excluding* the number sign (#), semicolon (;), and comma (,). The default is undefined.
Authentication traps	Enables or disables authentication trap generation in response to authentication failures. The default is disabled.

SNMP Trap Configuration

SNMP trap configuration supports setting up to eight trap destinations. Choose from Traps 1–Trap 8 to configure each trap. Table D-2 describes the parameters for configuring a SNMP trap.

Table D-2. SNMP Trap Configuration Parameters

Parameter	Description
Trap *n* enabled	Enables or disables trap *n*. If disabled, the trap is not configured.
Trap address*	Specifies the IP address to which the SNMP traps are sent. A maximum of eight trap addresses are supported. The default address for traps is 0.0.0.0.
Trap port*	The port number on which the trap is sent. The default is 162.
Trap version	Specifies the SNMP version (1 or 2) with which to format traps.

Table Notes

*Trap address (other than 0.0.0.) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and trap 2 have the same port value, they must have different addresses.

Management Information Base (MIB)

The following sections describe the QLogic management information base (MIB). The MIB consists of four object groups:

- System Information
- Network Port Table
- Fibre Channel Port Table
- Fibre Channel Port Table

System Information

The system information objects provide the system serial number, version numbers (hardware/software/agent), and number of ports (FC/GE).

qsrSerialNumber

Syntax	SnmpAdminString
Access	Read only
Description	The system serial number.

qsrHwVersion

Syntax	SnmpAdminString
Access	Read only
Description	The system hardware version number.

qsrSwVersion

Syntax	SnmpAdminString
Access	Read only
Description	The system software (firmware) version number.

qsrNoOfFcPorts

Syntax	Unsigned32
Access	Read only
Description	The number of Fibre Channel ports on the system.

qsrNoOfGbEPorts

Syntax	Unsigned32
Access	Read-only
Description	The number of gigabit Ethernet ports on the system.

qsrAgentVersion

Syntax	SnmpAdminString
Access	Read only
Description	The version number of the agent software on the system.

Network Port Table

The network port table contains a list of network ports that are operational on the router. The entries in this table include the management port, the iSCSI ports, and the TOE ports on the router. A single gigabit Ethernet port can function as an iSCSI port and a TOE simultaneously; therefore, there may be up to two entries for a given gigabit Ethernet port.

qsrNwPortTable

Syntax	**Sequence of** QsrNwPortEntry
Access	Not accessible
Description	The entries in this table include the management port, and the iSCSI, and TOE ports on the router.

qsrNwPortEntry

Syntax	QsrNwPortEntry
Access	Not accessible
Description	Each entry (row) contains information about a specific network port.

QsrNwPortEntry

A network port entry consists of the following sequence of objects:

qsrNwPortRole	QsrPortRole
qsrNwPortIndex	unsigned32
qsrNwPortAddressMode	INTEGER
qsrIPAddressType	InetAddressType
qsrIPAddress	InetAddress

qsrNetMask	InetAddress
qsrGateway	InetAddress
qsrMacAddress	MacAddress
qsrNwLinkStatus	QsrLinkStatus
qsrNwLinkRate	QsrLinkRate

qsrNwPortRole

Syntax	QsrPortRole
Access	Not accessible
Description	The operational role of this port: management port, iSCSI port, a TOE.

qsrNwPortIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer indexing each network port in a given role.

qsrNwPortAddressMode

Syntax	INTEGER 1 = Static 2 = DHCP 3 = Bootp 4 = RARP
Access	Read only
Description	The method by which the port gets its IP address.

qsrIPAddressType

Syntax	InetAddressType
Access	Read only
Description	The IP address type: ipv4 or ipv6.

qsrIPAddress

Syntax	InetAddress
Access	Read only
Description	The IP address of the port.

qsrNetMask

Syntax	InetAddress
Access	Read only
Description	The subnet mask for this port.

qsrGateway

Syntax	InetAddress
Access	Read only
Description	The gateway for this port.

qsrMacAddress

Syntax	IMacAddress
Access	Read only
Description	The MAC address for this port.

qstNwLinkStatus

Syntax	QsrLinkStatus
Access	Read only
Description	The operational link status for this port.

qsrNwLinkRate

Syntax	QsrLinkRate
Access	Read only
Description	The operational link rate for this port.

Fibre Channel Port Table

This table contains a list of the Fibre Channel (FC) ports on the router.There are as many entries in this table as there are FC ports on the router.

qsrFcPortTable

Syntax	**Sequence of** QsrFcPortEntry
Access	Not accessible
Description	A list of the FC ports on the router.There are as many entries in this table as there are FC ports on the router.

qsrFcPortEntry

Syntax	QsrFcPortEntry
Access	Not accessible
Description	Each entry (row) contains information about a specific FC port.

QsrFcPortEntry

A fibre channel port entry consists of the following sequence of objects:

qsrFcPortRole	QsrPortRole
qsrFcPortIndex	Unsigned32
qsrFcPortNodeWwn	PhysAddress
qsrFcPortWwn	PhysAddress
qsrFcPortId	PhysAddress
qsrFcPortType	Unsigned32
qsrFcLinkStatus	QsrLinkStatus
qsrFcLinkRate	QsrLinkRate

qsrFcPortRole

Syntax	QsrPortRole
Access	Not accessible
Description	The operational role of this port: FCP mode or frame shuttle mode.

qsrFcPortIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer indexing each FC port in a given role.

qsrFcPortNodeWwn

Syntax	PhysAddress
Access	Read only
Description	The world wide name of the node that contains this port.

qsrFcPortWwn

Syntax	PhysAddress
Access	Read only
Description	The world wide name for this port.

qsrFcPortId

Syntax	PhysAddress
Access	Read only
Description	The interface's 24-bit FC address identifier.

qsrFcPortType

Syntax	Unsigned32
Access	Read only
Description	The type of FC port, as indicated by the use of the appropriate value assigned by IANA. The IANA-maintained registry for FC port types can be found at: www.iana.org/assignments/fc-port-types

qsrFcLinkStatus

Syntax	QsrLinkStatus
Access	Read only
Description	The current link status for this port.

qsrFcLinkRate

Syntax	QsrLinkRate
Access	Read only
Description	The current link rate for this port.

Sensor Table

This table contains a list of all the sensors on the router. There are as many entries (rows) in this table as there are sensors.

qsrSensorTable

Syntax	**Sequence of** QsrSensorEntry
Access	Not accessible
Description	A list of all the sensors on the router. There are as many entries (rows) in this table as there are sensors.

qsrSensorEntry

Syntax	QsrSensorEntry
Access	Not accessible
Description	Each entry (row) corresponds to a single sensor.

QsrSensorEntry

A sensor entry consists of the following sequence of objects:

qsrSensorType	INTEGER
qsrSensorIndex	Unsigned32
qsrSensorUnits	INTEGER
qsrSensorValue	Integer32
qsrUpperThreshold	Integer32
qsrLowerThreshold	Integer32
qsrSensorState	INTEGER

qsrSensorType

Syntax	INTEGER Temperature = 1
Access	Not accessible
Description	The type of data being measured by this sensor.

qsrSensorIndex

Syntax	Unsigned32
Access	Not accessible
Description	A positive integer identifying each sensor of a given type.

qsrSensorUnits

Syntax	INTEGER Celsius = 1
Access	Read only
Description	The unit of measurement for the sensor.

qsrSensorValue

Syntax Integer32

Access Read only

Description The current value of the sensor.

qsrUpperThreshold

Syntax Integer32

Access Read only

Description The upper-level threshold for this sensor.

qsrLowerThreshold

Syntax Integer32

Access Read only

Description The lower-level threshold for this sensor.

qsrSensorState

Syntax INTEGER

Access Read only

Description The state of this sensor, indicating the health of the system.

- **Unknown –** The sensor value/thresholds cannot be determined.
- **Normal –** The sensor value is within normal operational limits.
- **Warning –** The sensor value is approaching a threshold.
- **Critical –** The sensor value has crossed a threshold.

Notifications

The router provides the following notification types:

- Notification Objects
- Agent Start Up Notification
- Agent Shut Down Notification
- Network Port Down Notification
- Fibre Channel Port Down Notification
- Sensor Notification
- Generic Notification

The following sections describe these notifications and objects they use.

Notification Objects

This section defines the objects used in notifications.

qsrEventSeverity

Syntax	INTEGER
Access	Accessible for notify
Description	This notification indicates the severity of the event. The value *clear* specifies that a condition that caused an earlier trap is no longer present.

qsrEventDescription

Syntax	SnmpAdminString
Access	Accessible for notify
Description	A textual description of the event that occurred.

qsrEventTimeStamp

Syntax	DateAndTime
Access	Accessible for notify
Description	This notification indicates when the event occurred.

Agent Start Up Notification

The agent startup notification indicates that the agent on the router has started running.

qsrAgentStartup uses the following object:

- qsrEventTimeStamp

Agent Shut Down Notification

The agent shut down notification indicates that the agent on the router is shutting down.

qsrAgentShutdown uses the following object:

- qsrEventTimeStamp

Network Port Down Notification

The network port down notification indicates that the specified network port is *down*. The next time the port comes up, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrNwPortDown uses the following objects:

- qsrNwLinkStatus
- qsrEventTimeStamp
- qsrEventSeverity

Fibre Channel Port Down Notification

The Fibre Channel port down notification indicates that the specified Fibre Channel port is *down*. The next time the port comes up, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrFcPortDown uses the following objects:

- qsrFcLinkStatus
- qsrEventTimeStamp
- qsrEventSeverity

Sensor Notification

The sensor notification indicates that the state for the specified sensor is not *normal*. When the sensor returns to the normal state, this event is sent with the *qsrEventSeverity* object set to *clear*.

qsrSensorNotification uses the following objects:

- qsrSensorValue
- qsrSensorState
- qsrEventTimeStamp
- qsrEventSeverity

Generic Notification

The generic notification reports events other than the defined event types. It provides a description object that identifies the event in clear text.

qsrGenericEvent uses the following objects:

- qsrEventTimeStamp
- qsrEventSeverity
- qsrEventDescription

Notes